ANNÉE UNIVERSITAIRE 2012/2013
Session 1 d'Automne

Master Sciences et Technologies, Mention Mathématiques ou Informatique

Spécialité Cryptologie et Sécurité Informatique

UE M1MA7W01 : Arithmétique

Responsable : Jean-Paul Cerri

Date : 17/12/2012 Durée : 3h

Exercice 1 – [Questions de cours]

1) Quels sont les sous-corps de $\mathbb{F}_{3^{12}}$? Représenter le diagramme des inclusions.

2) Quelle est la forme de la décomposition de $X^{11}-1$ dans $\mathbb{F}_3[X]$ (nombre de facteurs irréductibles et leurs degrés) ?

3) Quel est le nombre de polynômes unitaires irréductibles de degré 3 dans $\mathbb{F}_3[X]$?

4) Quel est le nombre de polynômes unitaires primitifs de degré 3 dans $\mathbb{F}_3[X]$?

Exercice 2 – [Corps $\mathbb{F}_{25}$]

1) On note A l'anneau $\dfrac{\mathbb{F}_5[X]}{(X^2+X+2)}$. Montrer que A est un corps.

2) Soit α la classe de X dans A. Calculer successivement α^2, α^4, α^8 et α^{12}.

3) Le polynôme X^2+X+2 est-il primitif dans $\mathbb{F}_5[X]$?

4) Quel est le polynôme minimal de α^2 sur $\mathbb{F}_5$? Est-il primitif ?

5) Même question avec α^7 à la place de α^2.

6) Dresser la liste des polynômes de degré 2, primitifs et unitaires de $\mathbb{F}_5[X]$.

Exercice 3 – [MLS]

1) Montrer que X^5+X^2+1 est irréductible dans $\mathbb{F}_2[X]$.

2) Soit $n \geqslant 2$ un entier tel que 2^n-1 soit premier. Montrer que n est nécessairement premier.

3) On suppose dans les questions **3**, **4**, **5**, **6** et **7** que 2^n-1 est premier. Rappeler pourquoi n divise 2^n-2.

4) Quel est le nombre de polynômes irréductibles de $\mathbb{F}_2[X]$ de degré n ?

5) Quel est le nombre de polynômes primitifs de $\mathbb{F}_2[X]$ de degré n ?

6) En déduire que tout polynôme irréductible de $\mathbb{F}_2[X]$ de degré n est en fait primitif.

7) Ne pouvait-on pas établir ce résultat directement, sans passer par un dénombrement ?

8) On considère la suite $(s_i)_{i\geqslant 0} \in (\mathbb{F}_2)^{\mathbb{N}}$ définie par la donnée de ses 5 premiers termes $s_0,\ s_1,\ s_2,\ s_3, s_4$ et par la relation de récurrence linéaire

$$s_{i+5} = s_{i+2} + s_i \quad \text{pour tout } i \geqslant 0.$$

Déterminer la matrice A associée à la suite, i.e. la matrice $A \in \mathcal{M}_{5\times 5}(\mathbb{F}_2)$ telle que pour tout $i \geqslant 0$ on ait

$$\begin{pmatrix} s_{i+1} \\ s_{i+2} \\ s_{i+3} \\ s_{i+4} \\ s_{i+5} \end{pmatrix} = A \begin{pmatrix} s_i \\ s_{i+1} \\ s_{i+2} \\ s_{i+3} \\ s_{i+4} \end{pmatrix}.$$

9) Déterminer son polynôme caractéristique $\chi_A(X)$.

10) Déduire de la question **6** que $(s_i)_{i\geqslant 0}$ est une MLS (maximal length sequence). Quelle est sa période ?

11) On pose $s_0 = 0,\ s_1 = 0,\ s_2 = 0,\ s_3 = 0,\ s_4 = 1$. Calculer les premiers termes de la suite et vérifier qu'il s'agit bien d'une MLS.

12) On garde les hypothèses de la question précédente. Soit α une racine de $\chi_A(X)$ dans $\mathbb{F}_{32}$. Écrire le terme général de la suite sous la forme $s_i = \mathrm{Tr}(\alpha^{i+k})$ où Tr désigne l'application trace de $\mathbb{F}_{32}$ dans $\mathbb{F}_2$ et où k est un entier naturel à déterminer.

Exercice 4 – [Code de Hamming]

1) On considère la matrice $M \in \mathcal{M}_{11\times 15}(\mathbb{F}_2)$ suivante :

$$M = \begin{pmatrix}
\mathbf{1} & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \mathbf{1} & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \mathbf{1} & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \mathbf{1} & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & 0 & 0 & \mathbf{1}
\end{pmatrix}.$$

On note L_i la ligne numéro i de M $(1 \leqslant i \leqslant 11)$. Expliquer pourquoi les L_i sont linéairement indépendantes sur $\mathbb{F}_2$.

2) On considère le code linéaire binaire C de longeur 15 admettant M comme matrice génératrice. Quel est le cardinal de C ?

3) Montrer que le mot

$$c = \begin{pmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & 0 & 0 \end{pmatrix}$$

appartient à C.

4) En déduire que C est cyclique.

5) Quel est le polynôme générateur de C ?

6) Montrer que C est un code de Hamming de longueur 15. Quels sont ses paramètres ?
7) Y a-t-il d'autres codes de Hamming de longueur 15 ? Si oui, exprimer leurs polynômes générateurs.
8) Soit $C^{\perp}$ le code dual de C. On sait qu'il est nécessairement cyclique. Quel est son polynôme générateur ?
9) Donner une matrice génératrice de $C^{\perp}$.

Exercice 5 – [Code de Reed-Solomon]

On considère le code de Reed-Solomon C défini sur $\mathbb{F}_7$ de longueur 6, de dimension 2 et de matrice génératrice

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{pmatrix}.$$

On a pris 5 pour élément primitif de $\mathbb{F}_7$.
1) Quels sont les paramètres de C ? Quel est l'ordre de sa capacité de décodage e ?
2) Un mot c est envoyé à l'aide du polynôme $P(X) \in \mathbb{F}_7[X]$ de degré < 2. On reçoit le mot

$$r = (r_1, r_2, r_3, r_4, r_5, r_6) = (5, 3, 0, 0, 1, 0),$$

qui contient au plus e erreurs. Calculer le polynôme interpolateur $R(X) \in \mathbb{F}_7[X]$ de degré $\leqslant 5$ qui vérifie

$$R(i) = r_i \quad \text{pour tout } 1 \leqslant i \leqslant 6.$$

3) À l'aide du début du développement en fraction continue de $\dfrac{R(X)}{X^6 - 1}$, retrouver $P(X)$ et le mot c.