UNIVERSITÉ de BORDEAUX

ANNÉE UNIVERSITAIRE 2016/2017
Session 1 d'Automne

Master Sciences et Technologies, Mention Mathématiques ou Informatique

Spécialité Cryptologie et Sécurité Informatique

UE 4TCY703U : Arithmétique

Responsable : M. Jean-Paul Cerri

Date : 14/12/2016. Durée : 3h.

Exercice 1 – Soient $P(X) = X^3 - X^2 + X + 1 \in \mathbb{F}_7[X]$ et $A = \dfrac{\mathbb{F}_7[X]}{\langle P(X) \rangle}$.

1) Montrer que $P(X)$ est produit de deux irréductibles unitaires de degrés 1 et 2, notés respectivement $R(X)$ et $S(X)$. L'anneau A est-il un corps ?

2) Quel est le cardinal de $A^\times$ le groupe des inversibles de A ?

3) Montrer que l'ordre de tout élément de $A^\times$ divise 48. Le groupe $A^\times$ est-il cyclique ?

4) Combien y a-t-il de polynômes unitaires irréductibles de degré 2 dans $\mathbb{F}_7[X]$?

5) Parmi ces polynômes combien sont primitifs ?

6) Montrer que $S(X)$ est primitif.

7) En déduire un élément de $A^\times$ d'ordre 48.

Exercice 2 – Soit p un nombre premier différent de 5. Considérons le polynôme $P(X) = X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_p[X]$.

1) Montrer que $5 \mid p^4 - 1$ et en déduire qu'il existe dans $(\mathbb{F}_{p^4})^\times$ un élément d'ordre 5 que l'on notera α.

2) Montrer que les racines de $P(X)$ dans $\mathbb{F}_{p^4}$ sont deux à deux distinctes et sont $\alpha, \alpha^2, \alpha^3, \alpha^4$.

3) Montrer que

- si $p \equiv 1 \bmod 5$, alors $\alpha \in \mathbb{F}_p$;
- si $p \equiv -1 \bmod 5$, alors $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$;
- si $p \equiv \pm 2 \bmod 5$, alors $\alpha \in \mathbb{F}_{p^4} \setminus \mathbb{F}_{p^2}$.

4) Donner suivant les trois cas la forme de la décomposition en produit d'irréductibles de $P(X)$ dans $\mathbb{F}_p[X]$.

5) Factoriser $P(X)$ dans $\mathbb{F}_{11}[X]$ et dans $\mathbb{F}_{19}[X]$.

6) On pose $\beta = \alpha + \alpha^{-1}$. Montrer que $(2\beta + 1)^2 = 5$.

7) En déduire que 5 est un carré dans $\mathbb{F}_p$ si et seulement si $p = 2$ ou $p \equiv \pm 1 \bmod 5$.

Exercice 3 – Soit $P(X) = X^4 - X - 1 \in \mathbb{F}_3[X]$.

1) Montrer que $P(X)$ est irréductible primitif. On identifie $\mathbb{F}_{81}$ et $\dfrac{\mathbb{F}_3[X]}{\langle P(X) \rangle}$ et on note α la classe de X dans $\mathbb{F}_{81}$.

2) Dresser la liste des classes cyclotomiques 3-aires modulo 40 et en déduire la forme de la factorisation de $X^{40} - 1$ dans $\mathbb{F}_3[X]$.

3) Montrer que dans $\mathbb{F}_3[X]$, $X^{40} - 1$ est le produit de $X - 1$, $X + 1$, de tous les irréductibles unitaires de degré 2 et de 8 irréductibles unitaires non primitifs de degré 4.

4) En déduire que $X^{40} + 1$ est produit de 10 irréductibles unitaires de degré 4, parmi lesquels 2 ne sont pas primitifs. Notons les $R(X)$ et $S(X)$.

5) Prouver que les racines de $R(X)$ et $S(X)$ dans $\mathbb{F}_{81}$ sont exactement les éléments de $(\mathbb{F}_{81})^\times$ d'ordre 16 et les exprimer comme puissances de α, en séparant les racines de $R(X)$ et celles de $S(X)$.

6) Montrer qu'il n'y a qu'un sous-corps K de $\mathbb{F}_{81}$ vérifiant $\mathbb{F}_3 \subsetneq K \subsetneq \mathbb{F}_{81}$. Exprimer ses éléments comme ploynômes en α de degrés < 4.

Exercice 4 – On considère la matrice de $M_{4\times 15}(\mathbb{F}_2)$ suivante :

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

1) Vérifier que les 4 lignes de G sont des vecteurs linéairement indépendants de $(\mathbb{F}_2)^{15}$.

2) On note $\mathcal{C}$ le code binaire linéaire de matrice génératrice G. Quel est le nombre de mots de $\mathcal{C}$?

3) Soit $\mathcal{C}^\perp$ le code dual de $\mathcal{C}$. Montrer que $(1,1,1,1,1,1,1,1,1,1,1,1,1,1,1) \in \mathcal{C}^\perp$ et en déduire que tous les mots de $\mathcal{C}$ sont de poids pair.

4) Montrer que $(1,0,0,0,1,1,1,1,0,1,0,1,1,0,0) \in \mathcal{C}$ et en déduire que le code $\mathcal{C}$ est cyclique.

5) Quel est son polynôme générateur ?

6) On se propose dans cette question de prouver que tout mot non nul de $\mathcal{C}$ est de poids 8.

(a) Montrer que $x \in \mathcal{C} \Leftrightarrow \exists\, u \in \mathbb{F}_2^4$ tel que $x = uG$.

(b) Soient $u \in \mathbb{F}_2^4$, $u \neq (0,0,0,0)$ et $f : \mathbb{F}_2^4 \to \mathbb{F}_2$ définie par $f(y) = \sum_{i=1}^4 u_i y_i$. Montrer que f est linéaire et que $|\operatorname{Ker} f| = 8$.

(c) En remarquant que les colonnes de G sont tous les vecteurs non nuls de $\mathbb{F}_2^4$, montrer que si $x \in \mathcal{C}$ est non nul, alors $\omega(x) = 8$.

7) Quels sont les paramètres de $\mathcal{C}$? Le code $\mathcal{C}$ est-il un code MDS ?

8) Que vaut e l'ordre de la condition de décodage vérifiée par $\mathcal{C}$?

9) On sait par le cours que $\mathcal{C}^\perp$ est également cyclique. Quel est le polynôme générateur de $\mathcal{C}^\perp$? En déduire une matrice de contrôle de $\mathcal{C}$.

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

11) On envoie un mot $c \in \mathcal{C}$ et le mot reçu est $r = (1,0,1,0,1,1,0,0,1,0,0,0,0,0,0)$. On admet qu'il y a au plus e erreurs dans r. Retrouver c.

Exercice 5 –

1) Montrer que tout polynôme irréductible de degré 7 de $\mathbb{F}_2[X]$ est primitif.

2) Montrer que $P(X) = X^7 + X + 1 \in \mathbb{F}_2[X]$ est irréductible primitif. On identifie $\mathbb{F}_{128}$ et $\dfrac{\mathbb{F}_2[X]}{\langle P(X)\rangle}$.

3) Montrer que $P(X)$ divise $X^{127} - 1$ dans $\mathbb{F}_2[X]$.

4) Soit $\mathcal{C}$ le code binaire cyclique de longueur 127 engendré par $P(X)$. Quels sont les paramètres de $\mathcal{C}$?

5) Soit $(s_i)_{i\geqslant 0} \in (\mathbb{F}_2)^{\mathbb{N}}$ la suite définie par $(s_0, s_1, s_2, s_3, s_4, s_5, s_6) = (1,1,1,1,1,0,0)$ et par la relation $s_{i+7} = s_{i+1} + s_i$ pour tout $i \geqslant 0$. Montrer que $(s_i)_{i\geqslant 0}$ est périodique et déterminer sa période r.

6) Soit α la classe de X dans $\mathbb{F}_{128}$.

a) Calculer $\mathrm{Tr}(1)$ et expliquer pourquoi $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\alpha^2) = \mathrm{Tr}(\alpha^4) = 0$.

b) Exprimer α^{12} et α^{24} comme polynômes en α de degrés < 7 et en déduire $\mathrm{Tr}(\alpha^5)$ et $\mathrm{Tr}(\alpha^3)$.

c) Donner la valeur de $\mathrm{Tr}(\alpha^i)$, pour $0 \leqslant i \leqslant 6$.

d) Rappeler pourquoi il existe un entier $k \geqslant 0$ tel que $s_i = \mathrm{Tr}(\alpha^{i+k})$ pour tout $i \geqslant 0$ et déterminer k en calculant les premiers termes de $(s_i)_{i\geqslant 0}$.

7) On considère le code $\mathcal{C}'$ constitué par le r-uplet nul et les r-uplets $(s_n, s_{n+1}, \ldots, s_{n+r-1})$ $(0 \leqslant n \leqslant r-1)$. Montrer que $\mathcal{C}'$ est linéaire cyclique.

8) Quelle est la dimension de $\mathcal{C}'$?

9) Quel est l'ordre de la condition de décodage de $\mathcal{C}'$?

10) Montrer que $P(X) \in \mathcal{C}'^\perp$ et en déduire que $\mathcal{C}' = \mathcal{C}^\perp$.