UNIVERSITÉ de BORDEAUX

ANNÉE UNIVERSITAIRE 2015/2016

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 : 15/12/2015. Durée : 3h.

Exercice 1 – Soit p un nombre premier.

1) On se propose d'abord de démontrer que X^4+1 n'est pas irréductible dans $\mathbb{F}_p[X]$.

a) Examiner le cas $p=2$.

On suppose désormais que $p>2$.

b) Montrer que $8 \mid p^2-1$.

c) En déduire qu'il existe dans $\mathbb{F}_{p^2}^\times$ un élément d'ordre 8.

d) Établir que dans $\mathbb{F}_{p^2}[X]$, le polynôme X^8-1 est scindé à racines simples.

e) En déduire que X^4+1 a toutes ses racines dans $\mathbb{F}_{p^2}$ et conclure.

2) Cherchons à préciser les choses. En s'inspirant de ce qui précède, montrer que si $p=2$ ou $p \equiv 1 \bmod 8$, dans $\mathbb{F}_p[X]$ le polynôme X^4+1 est scindé (à racines simples si $p \neq 2$), et que sinon, il est produit de deux irréductibles de degré 2 de $\mathbb{F}_p[X]$.

3) Factoriser X^4+1 dans $\mathbb{F}_3[X]$ et dans $\mathbb{F}_{17}[X]$.

Soit maintenant p un premier *impair* et soit $P(X)$ un diviseur irréductible de X^4+1 dans $\mathbb{F}_p[X]$. Soit d son degré. On note K le corps $\mathbb{F}_p[X]/(P(X))$ et α la classe de X dans K.

4) Quelle est la caractéristique de K ? Quel est son cardinal ?

5) Montrer que $\alpha \in K^\times$ et que $(\alpha+\alpha^{-1})^2=2$.

6) Montrer que 2 est un carré dans $\mathbb{F}_p$, i.e. il existe $x \in \mathbb{F}_p$ tel que $2=x^2$, si et seulement si $\alpha+\alpha^{-1} \in \mathbb{F}_p$.

7) Montrer que $\alpha^3+\alpha^{-3} \neq \alpha+\alpha^{-1}$.

8) En déduire que 2 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \bmod 8$.

Exercice 2 –

1) Soit $P(X) \in \mathbb{F}_5[X]$ défini par $P(X)=X^3+X^2+2X+2$. Factoriser $P(X)$ dans $\mathbb{F}_5[X]$ et en déduire que l'anneau $A=\mathbb{F}_5[X]/(P(X))$ n'est pas un corps.

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

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

4) Soit $Q(X) \in \mathbb{F}_5[X]$ défini par $Q(X)=X^3+X^2+2$. Montrer que l'anneau $B=\mathbb{F}_5[X]/(Q(X))$ est un corps.

5) Combien y a-t-il de polynômes unitaires irréductibles de degré 3 dans $\mathbb{F}_5[X]$?

6) Combien y a-t-il de polynômes unitaires irréductibles primitifs de degré 3 dans $\mathbb{F}_5[X]$?

7) Le polynôme $Q(X)$ est-il primitif ? *Indication* : si α est la classe de X dans B, on pourra calculer α^4 puis α^{62} en se servant de l'automorphisme de Frobenius.

8) Soit d un entier naturel divisant $|B^\times|$. Combien y a-t-il dans $B^\times$ d'éléments d'ordre d ? Exprimer ces éléments en fonction de α.

Exercice 3 –

1) Soit $P(X) = X^6 + X^5 + X^2 + X + 1 \in \mathbb{F}_2[X]$. Effectuer les divisions euclidiennes dans $\mathbb{F}_2[X]$ de $P(X)$ par $X^2 + X + 1$, $X^3 + X + 1$ et $X^3 + X^2 + 1$.

2) En déduire que $P(X)$ est irréductible dans $\mathbb{F}_2[X]$. On identifie $\mathbb{F}_{64}$ à $\mathbb{F}_2[X]/(P(X))$.

3) Quels sont les sous-corps de $\mathbb{F}_{64}$?

4) Soit α la classe de X dans $\mathbb{F}_{64}$. Montrer que $\alpha^5 + \alpha^3 + \alpha^2$ appartient à un sous-corps strict K de $\mathbb{F}_{64}$. Exprimer les éléments de K comme polynômes en α de degrés inférieurs strictement à 6.

5) Montrer que $\alpha^3 + \alpha^2$ appartient à un sous-corps strict L de $\mathbb{F}_{64}$. Exprimer les éléments de L comme polynômes en α de degrés inférieurs strictement à 6.

6) Soit $(s_i)_{i\geqslant 0} \in (\mathbb{F}_2)^{\mathbb{N}}$ définie par $s_0 = s_1 = s_2 = s_3 = s_4 = 0$, $s_5 = 1$ et par la relation

$$s_{i+6} = s_{i+5} + s_{i+2} + s_{i+1} + s_i \quad \text{(pour tout } i \geqslant 0\text{)}.$$

Expliquer pourquoi $(s_i)_{i\geqslant 0}$ est périodique de période $r \leqslant 63$.

7) Calculer les premiers termes de $(s_i)_{i\geqslant 0}$ et en déduire r.

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

9) Rappeler pourquoi $P(X)$ divise $X^{63} - 1$ dans $\mathbb{F}_2[X]$.

10) Soit $\mathcal{C}$ le code binaire cyclique de longueur 63 et de polynôme générateur $P(X)$. Quelle est la dimension de $\mathcal{C}$? Quel est son cardinal ?

11) Quels sont les paramètres de $\mathcal{C}$?

12) Calculer α^8 et α^{11} comme polynômes en α de degrés inférieurs strictement à 6. En déduire un élément non nul de $\mathcal{C}$ de poids minimum.

Exercice 4 –

1) Montrer que dans $\mathbb{F}_8$, tout élément distinct de 0 et 1 est un élément primitif.

2) Expliquer pourquoi dans $\mathbb{F}_8[X]$ le polynôme $X^3 + X + 1$ est scindé à racines simples. Soit α une de ses racines dans $\mathbb{F}_8$.

3) On considère dans $\mathcal{M}_{3,7}(\mathbb{F}_8)$ la matrice

$$M = \begin{pmatrix} \alpha^2+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \alpha^2 & 1 & 0 & 0 \\ 0 & \alpha^2+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \alpha^2 & 1 & 0 \\ 0 & 0 & \alpha^2+1 & \alpha^2+\alpha+1 & \alpha^2+\alpha+1 & \alpha^2 & 1 \end{pmatrix}.$$

Montrer que les lignes de cette matrice sont linéairement indépendantes sur $\mathbb{F}_8$.

4) Soit $\mathcal{C}$ le code linéaire de matrice génératrice M. Quel est le cardinal de C ?

5) Montrer que $(1, 0, 0, \alpha^2+1, \alpha^2+\alpha+1, \alpha^2+\alpha+1, \alpha^2) \in \mathcal{C}$ et en déduire que $\mathcal{C}$ est cyclique.

6) Quel est le polynôme générateur $g(X)$ de $\mathcal{C}$?

7) Vérifier que $g(X) = (X-1)(X-\alpha)(X-\alpha^2)(X-\alpha^3)$ et en déduire que l'on a bien $g(X) \mid X^7 - 1$ dans $\mathbb{F}_8[X]$.

8) Soit $c = (c_0, c_1, c_2, c_3, c_4, c_5, c_6)$ un mot non nul de $\mathcal{C}$. Montrer que si $P(X) = \sum_{i=0}^{6} c_i X^i \in \mathbb{F}_8[X]$, on a $P(1) = P(\alpha) = P(\alpha^2) = P(\alpha^3) = 0$.

9) En déduire que $\omega(c) > 4$.

10) Quelle est la distance minimale de $\mathcal{C}$? Quel est l'ordre de la condition de décodage de $\mathcal{C}$ (le nombre d'erreurs que l'on peut corriger) ?

11) Soit $\mathcal{C}^\perp$ le dual de $\mathcal{C}$. Quel est le cardinal de $\mathcal{C}^\perp$?

12) On sait par le cours que $\mathcal{C}^\perp$ est un code cyclique. Quel est son polynôme générateur ?

13) Quelle est la distance minimale de $\mathcal{C}^\perp$?