Master CSI 1 2009-2010

Arithmétique : MHT 711

Examen du 14 décembre 2009

Master Sciences et Technologies, mention Mathématiques ou Informatique, spécialité Cryptologie et Sécurité informatique

Durée : 3 heures. Sans document.

Responsable : Gilles Zémor

Les exercices sont indépendants.

– Exercice 1.

a) On considère l'anneau $A = \mathbb{F}_5[X]/(X^2-1)$. Combien A contient-il d'éléments ?

b) Soit A^* le groupe des éléments inversibles de A. Combien A^* contient-il d'éléments ?

c) Quelle est la caractéristique de l'anneau A ?

d) Montrer que pour tout $a \in A^*$ on a $a^5 = a$ et en déduire $a^4 = 1$. le groupe $(A^*, \times)$ est-il cyclique ?

– Exercice 2.

a) Montrer que l'ensemble E des racines de $X^9 + X^3 + X$ dans le corps $\mathbb{F}_{27}$ est un espace vectoriel sur $\mathbb{F}_3$.

b) Combien E contient-il d'éléments ?

– Exercice 3. On considère la suite d'éléments de $\mathbb{F}_2$ définie par $a_0 = 0, a_1 = 1, a_2 = 1$ et la récurrence linéaire $a_{i+3} = a_{i+1} + a_i$. Écrire cette suite sous la forme algébrique $a_i = \mathrm{Tr}(\alpha^{i+k})$ où Tr() désigne l'application trace de $\mathbb{F}_8$ dans $\mathbb{F}_2$ et où k est un entier à déterminer.

– Exercice 4.

a) Montrer que le polynôme $X^5 + X^2 + 1$ est irréductible dans $\mathbb{F}_2[X]$. Est-il primitif ?

b) Soit α une racine de $X^5 + X^2 + 1$ dans $\mathbb{F}_{32}$. Trouver le polynôme minimal de α^3.

c) Que vaut la période de la suite binaire $(a_i)_{i \geqslant 0}$ où $a_i = \mathrm{Tr}(\alpha^i)$, Tr() désignant l'application trace de $\mathbb{F}_{32}$ dans $\mathbb{F}_2$? Donner une relation de récurrence linéaire satisfaite par la suite (a_i).

d) Trouver les cinq premiers termes a_0, a_1, a_2, a_3, a_4 de la suite (a_i).

– EXERCICE 5. Démontrer que $X^{19}+1$ a exactement deux facteurs irréductibles dans $\mathbb{F}_2[X]$.

– EXERCICE 6. À tout 15-uple binaire $\mathbf{v} = (v_0, v_1, \ldots, v_{14})$ on associe le polynôme $\mathbf{v}(X) = v_0 + v_1 X + \cdots + v_{14} X^{14}$.

a) Soit $g(X) = X^5 + X^4 + X^2 + 1 = (1+X)(1+X+X^4)$. Montrer que l'ensemble des 15-uples $\mathbf{v}$ tels que $\mathbf{v}(X)$ est un multiple de $g(X)$ est un code cyclique C de longueur 15.

b) Combien le code C contient-il de mots ?

c) Montrer que le vecteur (101001101001011) est un mot du code C.

d) Montrer que tous les mots de C sont de poids pair.

e) Soit α une racine de $1+X+X^4$ dans $\mathbb{F}_{16}$. Montrer que α est d'ordre 15.

f) Montrer que tout mot de code $\mathbf{v}$ est tel que le polynôme associé $\mathbf{v}(X)$ a α comme racine.

g) Montrer que tout polynôme de degré $\leqslant 14$ de la forme $X^i + X^j$ n'a pas α comme racine.

h) En déduire que la distance minimale de C est égale à 4.