Master CSI 2 2007-2008

Arithmétique : MHT 711

Examen du 15 décembre 2008

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. Utiliser ce que vous savez des facteurs irréductibles de $X^{63}+1$ dans $\mathbb{F}_2[X]$ pour en déduire le nombre de polynômes irréductibles de degré 6 sur $\mathbb{F}_2$. Combien de ces polynômes sont primitifs ?

– **Solution.** Il y a 9 polynômes irréductibles de degré 6 et $\phi(63)/6 = 6$ d'entre eux sont primitifs.

– EXERCICE 2. Soit A l'anneau $\mathbb{F}_3[X]/((X-1)^3)$. Combien A contient-il d'éléments ?

a) Combien y a-t-il de polynômes unitaires de degré 1 sur $\mathbb{F}_3$ qui n'ont pas 1 comme racine ?

b) En déduire le nombre de polynômes *réductibles* unitaires de degré 2 sur $\mathbb{F}_3$ qui n'ont pas 1 comme racine.

c) Combien y a-t-il de polynômes *irréductibles* unitaires de degré 2 sur $\mathbb{F}_3$?

d) En déduire le nombre d'éléments de l'anneau des inversibles A^* de A.

e) Montrer que pour tout élément α de A^* on a $\alpha^3 \in \mathbb{F}_3$ et $\alpha^6 = 1$. Vérifier que le cardinal de A^* que vous avez trouvé précédemment est bien un multiple de 6.

– **Solution.** $|A| = 27$.

a) 2.

b) 3.

c) $9 - 6 = 3$.

d) $|A^*| = 2(1+2+3+3) = 18$.

e) Si β est la classe de X modulo $(X-1)^3$, tout α s'écrit $a\beta^2+b\beta+c$, $a,b,c \in \mathbb{F}_3$. On a $\alpha^3 = a\beta^6 + b\beta^3 + c$ avec $\beta^3 = 1$.

– Exercice 3. Soit α un élément de $\mathbb{F}_8$ de polynôme minimal $X^3 + X + 1$. Trouver les puissances α^i de α qui sont de trace nulle.

– **Solution.** $\alpha, \alpha^2, \alpha^4$.

– Exercice 4.

a) Montrer que $X^5 + X^3 + X^2 + X + 1$ est un polynôme irréductible de $\mathbb{F}_2[X]$. Montrer, sans faire de calcul, qu'il est également primitif.

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

– **Solution.**

a) il est primitif car 31 est premier.

b) $P_{\alpha^2}(X) = P_\alpha(X) = X^5+X^3+X^2+X+1$. $P_{\alpha^3}(X) = X^5+X^4+X^3+X+1$.

– Exercice 5. Combien de facteurs irréductibles dans $\mathbb{F}_2[X]$ a le polynôme $X^{17} + 1$? Quels sont leurs degrés ?

– **Solution.** Il a 3 facteurs irréductibles de degrés $1, 8, 8$.

– Exercice 6. Montrer que le polynôme $1 + x^3 + x^6$ est le polynôme générateur d'un code cyclique binaire de longueur 9. Quelle est la dimension de code ? Quelle est sa distance minimale ?

– **Solution.** On sait que $1 + x + x^2$ divise $1 + x^3$ donc $1 + x^3 + x^6 = 1 + x^3 + (x^3)^2$ divise $1 + (x^3)^3 = 1 + x^9$. La dimension du code est $9 - 6 = 3$. Sa distance minimale est 3 (écrire tous les mots).

– Exercice 7. Soit la matrice

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

et soit C le code linéaire sur $\mathbb{F}_2$ de matrice génératrice $\mathbf{G}$.

a) Trouver une autre matrice génératrice de $\mathbf{G}$ sous forme systématique, c'est-à-dire commençant par la matrice identité 4×4.

b) En déduire une matrice de parité $\mathbf{H}$ de C.

c) En déduire la distance minimale de C.

d) Soit $\mathbf{x} = [100011100]$ un vecteur de $\mathbb{F}_2^9$. Calculer son syndrome et en déduire le mot de C le plus proche pour la distance de Hamming.

e) Quels sont les paramètres (longueur, dimension, distance minimale) du code dual $C^\perp$ de C ?

– Exercice 8. Soit (a_i) la suite définie par $a_0 = a_1 = a_2 = a_3 = 1$ et la récurrence linéaire :

$$a_i = a_{i-1} + a_{i-4}$$

pour $i \geqslant 4$.

a) Quelle est la période π de cette suite ?

b) Montrer que l'ensemble C constitué du π-uple $(a_0 a_1 \dots a_{\pi-1})$, de tous ces décalés circulaires, ainsi que du π-uple nul, est stable par addition dans $\mathbb{F}_2^\pi$.

c) En déduire qu'il s'agit d'un code cyclique. Trouver son polynôme générateur.

– **Solution.**

a) 15.

b) C'est parce que la période de a est maximale.

c) $g(X) = 1 + X + X^2 + X^3 + X^5 + X^7 + X^8 + X^{11}$.