Master CSI 1 2020-2021

Arithmétique : Examen du 17 décembre 2020

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

Responsable : Gilles Zémor

Durée : 3h. Sans document. Les exercices sont indépendants.

– Exercice 1. 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 $A^\times$ de A.

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

– Exercice 2.

a) Combien y a-t-il de polynômes irréductibles de degré 5 sur $\mathbb{F}_2$? (Justifier).

b) Utiliser la factorisation dans $\mathbb{F}_2[X]$ de $X^{64}+X$ pour compter le nombre de polynômes irréductibles de degré 6 sur $\mathbb{F}_2$. Combien de ces polynômes sont primitifs ?

– Exercice 3.

a) Montrer que le polynôme $X^2 - X - 1$ est irréductible primitif sur $\mathbb{F}_3$.

b) Soit α une racine de X^2-X-1 dans $\mathbb{F}_9$. Quelle est la factorisation de X^8-1 en polynômes irréductibles unitaires sur $\mathbb{F}_9$? Quelle est la factorisation de X^8-1 en polynômes irréductibles unitaires sur $\mathbb{F}_3$?

c) Quels sont les polynômes irréductibles primitifs unitaires de degré 2 dans $\mathbb{F}_3[X]$?

– Exercice 4. Combien de facteurs irréductibles sur $\mathbb{F}_2$ a le polynôme $X^{19}+1$?

– Exercice 5. Soit $g(X) = X^5+X^4+1 = (X^2+X+1)(X^3+X+1) \in \mathbb{F}_2[X]$. Quelle est la plus petite longueur n d'un code cyclique de polynôme générateur $g(X)$?

– EXERCICE 6. On considère les suites binaires (a_i) données par la récurrence linéaire sur $\mathbb{F}_2$:

$$a_i = a_{i-2} + a_{i-4} + a_{i-5} + a_{i-6}. \qquad (1)$$

a) Quel est le polynôme de rétroaction $h(X)$ de la récurrence ? Montrer que $h(X)$ est irréductible.

b) Soit K le corps $K = \mathbb{F}_2[X]/(h)$. Soit α la classe de X, en d'autres termes une racine de $h(X)$ dans K. Quel est l'ordre multiplicatif de α ?

c) Montrer que la suite binaire $(b_i)_{i\geqslant 0}$ définie par $a_i = \mathrm{Tr}(\alpha^i)$ vérifie la récurrence (1). Tr() désigne l'application trace de K sur $\mathbb{F}_2$.

d) Quelle est la période n de cette dernière suite (b_i) ?

e) Montrer que toutes les suites non nulles solutions de la récurrence (1) ont pour période n.

f) Combien y a-t-il de suites solutions de la récurrence (1) ? Montrer que l'ensemble de ces suites, tronquées sur une période n, forme un code cyclique C de longueur n. Quel est sa dimension ? Pouvez-vous donner un polynôme générateur $g(X)$ de ce code cyclique ?

g) Donner les racines de $g(X)$ en fonction de α ou de α^{-1}. En déduire que la distance minimale d de C vérifie $d \geqslant 6$.

h) Montrer qu'il suffit d'examiner 3 multiples de $g(X)$ dans $\mathbb{F}_2[X]/(X^n + 1)$ pour connaître tous les poids des mots de C.

i) Quels sont les différents poids des mots de C ? Quelle est la distance minimale de C ?