Master CSI 1 2024-2025

Arithmétique : Examen du 18 décembre 2024

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.

a) Montrer que l'ordre multiplicatif de 2 dans $\mathbb{Z}/49\mathbb{Z}$ est 21.

b) Quel est la décomposition en facteurs irréductibles de $X^7 + 1$ dans $\mathbb{F}_2[X]$?

c) En écrivant $X^{49} + 1 = (X^7)^7 + 1$, trouver la décomposition en facteurs irréductibles de $X^{49} + 1$ dans $\mathbb{F}_2[X]$. Justifier.

– EXERCICE 2.

a) Montrer que $X^6 + X^3 + 1$ est irréductible dans $\mathbb{F}_2[X]$.

b) Quel est l'ordre d'une racine γ de $X^6 + X^3 + 1$ dans $\mathbb{F}_{64}$?

c) Soit $\beta = \gamma + 1$. Calculer les valeurs de β^{2^i}, $i = 1, 2, \ldots 6$, et en déduire, en justifiant, que le polynôme minimal $P(X)$ de β est de degré 6.

d) Montrer que β est un élément primitif de $\mathbb{F}_{64}$.

e) Quel est le polynôme minimal $P(X)$ de β ?

– EXERCICE 3. On considère les suites binaires $(a_i)_{i \geqslant 0}$ engendrées par la récurrence linéaire

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

a) Quel est le polynôme de rétroaction $h(X)$ de cette récurrence ?

b) Montrer que X est d'ordre 21 dans $\mathbb{F}_2[X]/h(X)$.

c) En déduire que $h(X)$ est irréductible.

d) Quelle est la période de n'importe quelle suite non nulle vérifiant la récurrence (1) ?

e) Soit α une racine de $h(X)$ dans $\mathbb{F}_{64}$. Calculer $\mathrm{Tr}(\alpha)$ où $\mathrm{Tr}()$ désigne la trace de $\mathbb{F}_{64}$ sur $\mathbb{F}_2$.

f) Montrer que α^3 est dans le sous-corps à huit éléments de $\mathbb{F}_{64}$.

g) En déduire, sans faire de calcul supplémentaire et en utilisant la définition de $\mathrm{Tr}()$, que $\mathrm{Tr}(\alpha^3) = 0$.

h) Sans faire de calcul supplémentaire, en déduire la valeur de $\mathrm{Tr}(\alpha^5)$.

i) Donner les dix premiers symboles de la suite (a_i) définie par $a_i = \mathrm{Tr}(\alpha^i)$ (en commençant à a_0).

j) Calculer le polynôme minimal de $\beta = \alpha + 1$.

k) Montrer que β est un élément primitif de $\mathbb{F}_{64}$.

l) On considère la suite $(b_i)_{i \geqslant 0}$ définie par $b_i = a_i + a_{i+1}$, où la suite (a_i) est la suite définie en **i)**. Donner une expression de $b_i + a_{i+d}$ sous la forme d'une trace et en déduire que si b_i est une décalée de (a_i), alors β doit être une puissance de α. En déduire que (b_i) n'est pas une décalée de (a_i).

Pour les deux exercices suivants, α désigne un élément de $\mathbb{F}_{16}$ racine du polynôme $X^4 + X + 1$. Il sera utile de disposer du tableau suivant qui donne les valeurs des puissances successives de α.

1	α	α^2	α^3	α^4	α^5	α^6	α^7
1	α	α^2	α^3	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^3+\alpha^2$	$\alpha^3+\alpha+1$
α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	α^{15}
α^2+1	$\alpha^3+\alpha$	$\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+\alpha$	$\alpha^3+\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+1$	α^3+1	1

– EXERCICE 4. Soit C le code cyclique de longueur 15 de polynôme générateur $g(X) = X^4 + X + 1$.

a) Quelle est la dimension et la distance minimale de ce code ?

b) En notation polynomiale, on considère le mot $\mathbf{y} = X + X^4 + X^8 + X^{10}$. Le mot $\mathbf{y}$ appartient-il au code C ? Sinon, quel est le mot de C le plus proche ?

– EXERCICE 5. Le but de l'exercice est de trouver le polynôme de $\mathbb{F}_2[X]$, de poids 2, $P(X) = X^i + X^j$, $0 \leqslant i, j \leqslant 14$, tel que

$$P(\alpha) = \alpha$$
$$P(\alpha^3) = \alpha^2 + 1$$

a) Poser $\alpha^i = x$ et $\alpha^j = y$, et utiliser l'identité $x^3 + y^3 = (x+y)(x^2 + xy + y^2)$ pour en déduire un système algébrique de la forme

$$x + y = a$$
$$xy = b$$

b) Trouver un polynôme $Q(X)$ de $\mathbb{F}_{16}[X]$ de degré 2 dont x et y sont racines.

c) Poser $x = x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3$ où $x_0, x_1, x_2, x_3 \in \mathbb{F}_2$. Transformer l'équation $Q(x) = 0$ en un système linéaire sur $\mathbb{F}_2$ d'inconnues x_0, x_1, x_2, x_3.

d) Résoudre le système. Quel est le polynôme $P(X) = X^i + X^j$?