Master CSI 1 — 2019-2020

Arithmétique : DS du 24 octobre 2019

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

Responsable : Gilles Zémor

Durée : 1h30. Sans document. Les exercices sont indépendants.

– EXERCICE 1. On considère l'anneau $A = \mathbb{F}_2[X]/(X^4 + X^2 + X + 1)$. Combien le groupe $(A^*, \times)$ contient-il d'éléments ? Est-ce un groupe cyclique ?

– EXERCICE 2.

a) Que pouvez-vous dire de la décomposition en facteurs irréductibles de $X^{27} - X$ sur $\mathbb{F}_3$? En déduire le nombre de polynômes irréductibles unitaires de degré 3 dans $\mathbb{F}_3[X]$.

b) Le polynôme $X^3 - X + 1$ est-il irréductible dans $\mathbb{F}_3[X]$? Est-il primitif ?

– EXERCICE 3. Soit $P(X) = X^5 - X - 1$ dans $\mathbb{F}_5[X]$. Soit x la classe de X dans l'anneau $A = \mathbb{F}_5[X]/(X^5 - X - 1)$.

a) Que valent x^5, x^{25}, x^{125} ? Plus généralement, quelles sont les valeurs prises par x^{5^n} dans A pour tous les entiers n ?

b) En déduire que $X^5 - X - 1$ est irréductible dans $\mathbb{F}_5[X]$.

– EXERCICE 4. On rappelle que le polynôme $X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$.

a) Montrer que le polynôme $X^2 + X + 1$ est irréductible sur $\mathbb{F}_8$.

b) Quels sont les entiers m pour lesquels le polynôme X^2+X+1 est irréductible sur $\mathbb{F}_{2^m}$?

c) Montrer que dans le corps $\mathbb{F}_{64}$ il existe un élément α tel que $\alpha^2 + \alpha + 1 = 0$ et un élément β tel que $\beta^3 + \beta + 1 = 0$.

d) Montrer que le polynôme minimal de $\alpha\beta$ est $X^6 + X^4 + X^2 + X + 1$.

e) Quel est l'ordre de $\alpha\beta$ dans $\mathbb{F}_{64}$? Le polynôme $X^6 + X^4 + X^2 + X + 1$ est-il primitif ?