Master CSI 1 2021-2022

Arithmétique : DS du 27 octobre 2021

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. Soit $A = \mathbb{F}_4[X]/(X^2 + X)$.

a) Combien l'anneau A contient-il d'éléments ? Combien d'éléments contient le groupe multiplicatif A^* des éléments inversibles de A ?

b) Combien d'éléments de A^* sont racines de $X^3 + 1$? Le groupe A^* est-il cyclique ?

– Exercice 2. Écrire $X^9 - X$ comme produit de polynômes irréductibles sur $\mathbb{F}_3$.

– Exercice 3. Soit $P(X) = X^6 + X^5 + X^3 + X^2 + 1$ dans $\mathbb{F}_2[X]$.

a) Calculer X^8 modulo $P(X)$, et en déduire rapidement que $P(X)$ est irréductible.

b) $P(X)$ est-il primitif ?

c) Soit α une racine de $P(X)$ dans $\mathbb{F}_{64}$. Quelles sont les puissances de α dont les polynômes minimaux ne sont pas de degré 6 ?

d) Trouver le polynôme minimal de α^3.

– Exercice 4. On considère le polynôme $P(X) = X^{2^m} + X + 1$.

a) Etudier les puissances de X modulo $P(X)$, et en déduire que les facteurs irréductibles de $P(X)$ dans $\mathbb{F}_2[X]$ ont un degré au plus $2m$.

b) Montrer que si m est une puissance de 2, alors $P(X)$ a un facteur irréductible de degré $2m$.

c) Remarquer que $P(X)$ est premier avec $X^{2^m} + X$ et en déduire que si m est premier, alors tous les facteurs irréductibles sur $\mathbb{F}_2$ de $P(X)$ sont de degré $2m$, sauf un qui est de degré 2.

– Exercice 5. Quels sont les degrés des polynômes irréductibles de $\mathbb{F}_4[X]$ qui divisent $X^{64} + X$? Comparer les décompositions de $X^{64} + X$ en produits de facteurs irréductibles sur $\mathbb{F}_2[X], \mathbb{F}_4[X]$ et $\mathbb{F}_{64}[X]$ pour en déduire qu'un polynôme irréductible de degré 6 dans $\mathbb{F}_2[X]$ n'est pas irréductible dans $\mathbb{F}_4[X]$.