# Master CSI 1 2022-2023

## Arithmétique : DS du 9 novembre 2022

*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 $A = \mathbb{F}_3[X]/(X^3+X)$.

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

**b)** Montrer que tout élément $\alpha$ de $A$ vérifie $\alpha^9 = \alpha$. En déduire que le groupe multiplicatif $A^*$ n'est pas cyclique.

– EXERCICE 2. Tous les polynômes considérés sont dans $\mathbb{F}_2[X]$.

**a)** Calculer $X^{2^i}$ modulo $X^7+X^3+1$, $i = 0,1,2,\ldots,7$ et en déduire que $X^7+X^3+1$ est irréductible.

**b)** Soit $P(X) = X^8+X^4+X^3+X+1 \in \mathbb{F}_2[X]$. On admettra que le plus petit entier $i \geqslant 1$ tel que $X^{2^i} = X \bmod P(X)$ vaut 8. Expliquer comment on peut en déduire que $P(X)$ est irréductible.

– EXERCICE 3. On considère $\mathbb{F}_{16}$, le corps à 16 éléments. Soit $\gamma$ un élément primitif de $\mathbb{F}_{16}$.

**a)** Quelles sont les puissances de $\gamma$, qui avec 0 et 1 constituent un sous-corps $K$ de $\mathbb{F}_{16}$ isomorphe à $\mathbb{F}_4$ ?

**b)** Montrer que pour tout $\alpha \in \mathbb{F}_{16}$, $\alpha + \alpha^4 \in K$.

**c)** Soit $\alpha \in \mathbb{F}_{16}$, $\alpha \notin K$. Que vaut $[\mathbb{F}_{16} : K]$ ?

**d)** En déduire le degré du polynôme minimal de $\alpha \notin K$ dans $K[X]$. Donner une expression des coefficients de ce polynôme minimal en fonction de $\alpha$.

– EXERCICE 4.

**a)** On considère le polynôme $X^6+X^3+1$ dans $\mathbb{F}_2[X]$. Calculer $X^{64}$ modulo $X^6+X^3+1$ et en déduire, en faisant très attention, que $X^6+X^3+1$ est irréductible.

**b)** $X^6+X^3+1$ est-il primitif ?

**c)** Soit $\alpha$ une racine de $X^6+X^3+1$ dans $\mathbb{F}_{64}$. Soit $\beta = \alpha^5+\alpha^2+\alpha$. Calculer $[\mathbb{F}_2(\beta) : \mathbb{F}_2]$.

**d)** Montrer que $\alpha+1$ est primitif.

**e)** Trouver le polynôme minimal de $\alpha+1$.