# Master CSI 1 — 2023-2024

## Arithmétique : DS du 25 octobre 2023

*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.

**a)** Montrer que dans $\mathbb{F}_{16}$ il existe un élément $\alpha \neq 1$ tel que $\alpha^5 = 1$.

**b)** Quel est le polynôme minimal de $\alpha$ ? De $\alpha + 1$ ?

– EXERCICE 2. Quels sont les entiers $m \geqslant 1$ pour lesquels le polynôme $X^2+X+1$ est irréductible dans $\mathbb{F}_{2^m}[X]$ ?

– EXERCICE 3. Tous les polynômes considérés sont dans $\mathbb{F}_2[X]$.

**a)** Quel est le pgcd de $X^8 + X + 1$ et $X^8 + X$ ?

**b)** Calculer $X^{2^6}$ modulo $X^8 + X + 1$.

**c)** Que peut-on déduire de **a)** et de **b)** sur les facteurs irréductibles de $X^8 + X + 1$ ?

**d)** Donner les facteurs irréductibles de $X^8 + X + 1$.

– EXERCICE 4. Soit $\mathbb{F}_q$ un corps fini. Montrer que si $a \in \mathbb{F}_q$, alors pour tout entier $n$, le polynôme $X^{q^n} - X + na$ est divisible par $X^q - X + a$ dans $\mathbb{F}_q[X]$. On pourra considérer les puissances successives de $X^q$ modulo $X^q - X + a$.

– EXERCICE 5. Soit $p$ un nombre premier et soit $k$ un diviseur de $p - 1$. Le but de l'exercice est de montrer que pour tout $a \in \mathbb{F}_p^*$, le polynôme $X^k - a$ a $k$ racines distinctes dans $\mathbb{F}_{p^k}$.

**a)** Pourquoi $k$ divise-t-il $p^k - 1$ ?

**b)** Calculer $p^i \bmod (p-1)$ et montrer que $k$ divise $1 + p + p^2 + \cdots + p^{k-1}$.

**c)** Montrer que le polynôme $X^k - 1$ a $k$ racines distinctes dans $\mathbb{F}_p$. On pourra les exprimer comme puissances d'un élément primitif $\alpha$ de $\mathbb{F}_p$.

**d)** En déduire que si $X^k - a$ a une racine dans $\mathbb{F}_{p^k}$, alors $X^k - a$ a $k$ racines distinctes dans $\mathbb{F}_{p^k}$.

**e)** On dira qu'un élément $b \in \mathbb{F}_{p^k}$ est une puissance $k$-ième si $b = c^k$ pour $c \in \mathbb{F}_{p^k}$. Montrer que les puissances $k$-ièmes de $\mathbb{F}_{p^k}^*$ sont de la forme $\beta^{ik}$ où $\beta$ est un élément primitif de $\mathbb{F}_{p^k}$. En déduire le nombre de puissances $k$-ièmes de $\mathbb{F}_{p^k}^*$.

**f)** En déduire que $x \in \mathbb{F}_{p^k}^*$ est une puissance $k$-ième si et seulement si $x$ est une racine de $X^{(p^k-1)/k} - 1$.

**g)** Montrer que $X^{p-1} - 1$ divise $X^{(p^k-1)/k} - 1$ dans $\mathbb{F}_p[X]$.

**h)** En déduire que si $a \in \mathbb{F}_p^*$, alors $a$ est une puissance $k$-ième dans $\mathbb{F}_{p^k}^*$.

**i)** Conclure.