Université Paris 8 Année 2022–2023

M2 Mathématiques et applications, parcours ACC

# Algorithmes arithmétiques II – Feuille de TD 5

20/10/2022

---

Le corrigé de certains exercices sera disponible à l'adresse suivante :
`www.math.univ-paris13.fr/~lavauzelle/teaching/2022-23/algorithmes-arithmetiques.html`
$(\star)$ exercice fondamental $(\star\star)$ pour s'entraîner $(\star\star\star)$ pour aller plus loin 💻 sur machine

---

## Exercice 1. $(\star)$ Irréductibilité et algèbre de Berlekamp.

Cet exercice est extrait de *Introduction to finite fields and applications*, Lidl & Niederreiter.

Soit $\mathbb{F}_q$ un corps fini et $\ell$ un nombre premier divisant $q-1$. Soit également $a \in \mathbb{F}_q^\times$. On souhaite montrer, à l'aide de l'algèbre de Berlekamp associée à $P(X) = X^\ell - a$, que l'on a

$$X^\ell - a \text{ est irréductible dans } \mathbb{F}_q[X] \quad \iff \quad a^{(q-1)/\ell} \neq 1\,.$$

**Question 1.–** Soit $0 \leq i < \ell$. Calculer $X^{iq} \bmod (X^\ell - a)$.

**Question 2.–** En déduire que l'algèbre de Berlekamp peut être décrite comme

$$\mathcal{B} = \ker \phi = \Big\{ \sum_{i=0}^{\ell-1} b_i X^i \;\mid\; b_i(a^{i(q-1)/\ell} - 1) = 0 \Big\}.$$

**Question 3.–** À l'aide des questions précédentes, démontrer le résultat souhaité.

## Exercice 2. $(\star)$ Polynôme irréductible sur les entiers, mais qui se factorise mod $p$.

On considère le polynôme $F(X) = X^4 + 1$. Notre but est de démontrer que $F(X)$ est irréductible dans l'anneau des polynômes à coefficients entiers, mais n'est dans aucun des anneaux $\mathbb{F}_p[X]$.

**Question 1.–** Démontrer que $f$ est irréductible dans $\mathbb{Q}[X]$, puis dans $\mathbb{Z}[X]$.

**Question 2.–** Factoriser $F(X)$ dans $\mathbb{F}_2[X]$.

Soit $p$ un premier impair.

**Question 3.–** Démontrer qu'il existe un élément $\alpha$ d'ordre 8 dans le groupe multiplicatif $\mathbb{F}_{p^2}^\times$. En déduire que $X - \alpha$ divise $F(X)$ dans $\mathbb{F}_{p^2}[X]$.

**Question 4.–** En raisonnant avec le conjugué de $\alpha$, démontrer que $F(X)$ admet une factorisation non-triviale dans $\mathbb{F}_p[X]$.