Université Paris 8 Année 2022–2023

M2 Mathématiques et applications, parcours ACC

Algorithmes arithmétiques II – Solutions feuille de TD 4

20/10/2022

Retrouvez le sujet du TD et d'autres exercices à l'adresse :

`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 ℓ 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

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

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.

Solutions de l'Exercice 1.

Solution Q1. On a :

$$X^{iq} = X^{i(q-1)}X^i = (X^\ell)^{i(q-1)/\ell}X^i \equiv a^{i(q-1)/\ell}X^i = \left(a^{(q-1)/\ell}X\right)^i \mod (X^\ell - a)\,.$$

Solution Q2. Rappelons que l'algèbre de Berlekamp $\mathcal{B}$ est le noyau de $\phi : B \mapsto B^q - B$ dans $\mathbb{F}_q[X]/(X^\ell - a)$. Pour $B \in \mathbb{F}_q[X]/(X^\ell - a)$, on calcule $B^q \mod (X^\ell - a)$:

$$B^q = \Big(\sum_{i=0}^{d} b_i X^i\Big)^q = \sum_{i=0}^{d} b_i^q X^{iq} \equiv \sum_{i=0}^{d} b_i a^{i(q-1)/\ell} X^i \mod (X^\ell - a)\,.$$

Donc

$$B \in \ker \phi \iff B^q - B \equiv 0 \mod (X^\ell - a) \iff \sum_{i=0}^{d} b_i(a^{i(q-1)/\ell} - 1)X^i \equiv 0 \mod (X^\ell - a)\,.$$

Comme $(1, \ldots, X^{\ell-1})$ est une base de $\mathbb{F}_q[X]/(X^\ell - a)$, on obtient

$$B \in \ker \phi \iff \forall i \in \{0, \ldots, \ell-1\},\, b_i(a^{i(q-1)/\ell} - 1) = 0\,.$$

Solution Q3. On a vu dans le cours l'équivalence

$$X^\ell - a \text{ irréductible} \iff \text{algèbre de Berlekamp } \mathcal{B} = \mathbb{F}_q$$

D'après **Q2.**, $\mathcal{B} = \{ \sum_{i=0}^{\ell-1} b_i X^i \mid b_i(a^{i(q-1)/\ell} - 1) = 0\}$, donc

$$X^\ell - a \text{ irréductible} \iff \forall i \in \{1, \dots, \ell-1\},\ a^{i(q-1)/\ell} - 1 \neq 0\,.$$

Remarquons enfin que, pour $i \in \{1, \dots, \ell-1\}$ fixé, on a

$$a^{i(q-1)/\ell} \neq 1 \iff a^{(q-1)/\ell} \neq 1,$$

car l'ordre de $a^{(q-1)/\ell}$ doit être un diviseur de ℓ, qui est premier. Ceci conclut la preuve.

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 α 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 α, démontrer que $F(X)$ admet une factorisation non-triviale dans $\mathbb{F}_p[X]$.

Solutions de l'Exercice 2.

Solution Q1. Pour tout $x \in \mathbb{Q}$, on a $x^4 + 1 \geq 1 > 0$ donc $F(X)$ n'admet pas de racine dans $\mathbb{Q}$. Si $F(X)$ est factorisable, alors c'est nécessairement comme produit de deux polynômes de degré 2. Notons les $P_1(X) = X^2 + a_1 X + b_1$ et $P_2(X) = X^2 + a_2 X + b_2$. Alors

$$F(X) = P_1(X)P_2(X) = X^4 + (a_1 + a_2)X^3 + (a_1a_2 + b_1 + b_2)X^2 + (b_1a_2 + b_2a_1)X + b_1b_2 \tag{1}$$

D'après le lemme de Gauss, comme $F(X)$ est primitif et à coefficients dans $\mathbb{Z}$, s'il est factorisable sur $\mathbb{Q}$, alors il l'est également sur $\mathbb{Z}$. L'expression (1) implique alors que $b_1b_2 = 1$ **dans les entiers relatifs**, on a :

$$\begin{cases} a_1 + a_2 = 0 \\ a_1a_2 + b_1 + b_2 = 0 \\ b_1a_2 + b_2a_1 = 0 \\ b_1b_2 = 1 \end{cases}$$

Par conséquent, $(b_1, b_2) \in \{(-1,-1), (1,1)\}$ puis $a_1a_2 \in \{-2, 2\}$. On a donc nécessairement $|a_1| \neq |a_2|$ (l'un vaut 1, l'autre vaut 2), ce qui est contradictoire avec $a_1 + a_2 = 0$.

Solution Q2. Sur $\mathbb{F}_2$, on a $X^4 + 1 = (X+1)^4$.

Solution Q3. Lorsque $p = 2k+1$ est impair, l'entier $p^2 - 1 = 4k^2 + 4k = 4k(k+1)$ est divisible par 8 (car k ou $k+1$ est pair). Par conséquent, si ω est un générateur de $\mathbb{F}_{p^2}^\times$ de cardinal $p^2 - 1$, alors $\alpha = \omega^{(p^2-1)/8}$ est d'ordre 8 dans ce groupe.

On observe alors que $\alpha^4 = -1$ (α^4 est une racine carrée de 1, qui ne peut pas être 1 sinon α aurait un ordre ≤ 4), donc $F(\alpha) = 0$. C'est équivalent au fait que $X - \alpha$ divise $F(X)$.

Solution Q4. Notons $\overline{\alpha}$ le conjugé de α dans $\mathbb{F}_{p^2}$, c'est-à-dire $\overline{\alpha} = \alpha^p$. Alors, on sait que $X - \overline{\alpha}$ divise également $F(X)$, donc

$$P(X) = (X - \alpha^p)(X - \alpha) = X^2 - \underbrace{(\alpha^p + \alpha)}_{\mathrm{Tr}(\alpha) \in \mathbb{F}_p} X + \underbrace{\alpha^{p+1}}_{\mathrm{N}(\alpha) \in \mathbb{F}_p}$$

est un polynôme à coefficients dans $\mathbb{F}_p$ qui divise $X^4 + 1$.