Université Paris 8 Année 2021–2022

M2 Mathématiques et applications, parcours ACC

Algorithmes arithmétiques II – Feuille de TD 4

13/10/2021

Le corrigé de certains exercices sera disponible à l'adresse suivante :

`www.math.univ-paris13.fr/~lavauzelle/teaching/2021-22/algorithmes-arithmetiques.html`

$(\star)$ exercice fondamental $(\star\star)$ pour s'entraîner $(\star\star\star)$ pour aller plus loin 💻 sur machine

---

Exercice 1. $(\star)$ Un critère de divisibilité.

Dans cet exercice, on considère un polynôme $P \in \mathbb{F}_q[X]$ irréductible. On souhaite démontrer le résultat suivant.

Pour tout $\ell \geq 1$,

$$P \text{ divise } X^{q^\ell} - X \iff \deg P \text{ divise } \ell\,.$$

Question 1.– Soit ℓ et d deux entiers tels que $\ell \mid d$. Démontrer que $q^\ell - 1$ divise $q^d - 1$.

Question 2.– Démontrer que si $\deg P$ divise ℓ, alors P divise $X^{q^\ell} - X$.

Question 3.– Démontrer que, pour tout polynôme $B(X) \in \mathbb{F}_q[X]$, on a $B(X)^{q^{\deg P}} \equiv B(X) \bmod P$.

Question 4.– En effectuant une division euclidienne de ℓ par $\deg P$, conclure.

Exercice 2. $(\star\star)$ Un test d'irréductibilité.

Dans cet exercice, on admet le résultat de l'Exercice 1 : pour tout polynôme $A \in \mathbb{F}_q[X]$ irréductible et pour tout $\ell \geq 1$,

$$A \text{ divise } X^{q^\ell} - X \iff \deg(A) \text{ divise } \ell\,.$$

On considère le polynôme $P(X) = X^{q^n} - X \in \mathbb{F}_q[X]$, où $n \geq 1$.

Question 1.– Calculer $P'(X)$. Le polynôme $P(X)$ contient-il des facteurs carrés ?

Question 2.– Démontrer que $P(X)$ est le produit de tous les polynômes irréductibles dont le degré divise n.

Question 3.– Soit $Q(X) \in \mathbb{F}_q[X]$ de degré d. Démontrer que $Q(X)$ est irréductible si et seulement si les deux conditions suivantes sont satisfaites :

1. $Q(X)$ divise $X^{q^d} - X$,
2. pour tout r diviseur strict de d, les polynômes $Q(X)$ et $X^{q^r} - X$ sont premiers entre eux.

Question 4.– En déduire un algorithme déterministe de test d'irréductibilité, et calculer sa complexité.

Exercice 3. ($\star\star$) Factorisation de polynômes en caractéristique 2.

L'objectif de cet exercice est de traiter le cas de la caractéristique 2 dans les algorithmes de Berlekamp et Cantor–Zassenhaus. Soit donc $q = 2^k$, et définissons pour un entier $m \geq 1$ quelconque l'application

$$T_m : x \mapsto x^{2^{m-1}} + x^{2^{m-2}} + \cdots + x^2 + x\,.$$

Question 1.– Démontrer que pour tout $A(X) \in \mathbb{F}_{2^k}[X]$, on a $A(X)^{2^m} + A(X) = T_m(A(X)) \cdot (T_m(A(X)) + 1)$.

Soit $P(X) \in \mathbb{F}_{2^k}[X]$ un polynôme.

Question 2.– Démontrer que si $B(X) \in \mathbb{F}_{2^k}[X]/(P)$ vérifie $B(X)^{2^m} \equiv B(X) \mod P$, alors $T_m(B(X))^2 \equiv T_m(B(X)) \mod P$.

On suppose maitenant que P est sans facteur carré. donc les facteurs irréductibles sont $P_1, \ldots, P_r \in \mathbb{F}_{2^k}[X]$. On note $\chi_i(F) \coloneqq F \mod P_i \in \mathbb{F}_{2^k}[X]/(P_i)$.

Question 3.– [Berlekamp] Démontrer pour tout polynôme B dans l'algèbre de Berlekamp $\mathcal{B}$, on a $\chi_i(T_k(B)) \in \mathbb{F}_2$. En déduire que si B est tiré uniformément dans $\mathcal{B}$, alors $T_k(B) \in \mathbb{F}_2$ avec probabilité 2^{1-r}.

Question 4.– [Cantor–Zassenhaus] On suppose que P est tel que les P_i ont même degré d. Démontrer que pour tout $A \in \mathbb{F}_q[X]/(P)$, on a $\chi_i(T_{kd}(A)) \in \mathbb{F}_2$. En déduire que si A est tiré uniformément dans $\mathbb{F}_q[X]/(P)$, alors $T_{kd}(A) \in \mathbb{F}_2$ avec probabilité 2^{1-r}.

Exercice 4. ($\star\star$) 💻 Implantation de l'algorithme de Berlekamp.

Dans cet exercice, on considère un polynôme $P \in \mathbb{F}_q[X]$ à factoriser.

Prérequis : avoir implanté des algorithmes de :

- calcul de pgcd dans $\mathbb{F}_q[X]$,
- calcul d'un élément non-nul du noyau d'une matrice,
- calcul d'exponentiation modulaire rapide sur les polynômes.

Question 1.– Implanter une fonction `squarefree_factorisation` qui prend en entrée un polynôme $P(X)$ quelconque, et retourne la partie sans carré de $P(X)$.

Question 2.– Implanter une fonction de `compute_matrix`, qui prend en entrée un polynôme sans carré $P(X)$ de degré n, et retourne la matrice de l'application $\mathbb{F}_q$–linéaire $\phi : A(X) \mapsto A(X)^q - A(X) \mod P(X)$ dans la base $(1, X, \ldots, X^{n-1})$.

Question 3.– Écrire une fonction `factorisation_berlekamp_small` qui implante l'algorithme de Berlekamp dans le cas q petit (c'est-à-dire, en énumérant le corps $\mathbb{F}_q$). Retrouver expérimentalement la complexité en $O(n^3 + n^2 q))$.

Question 4.– On suppose ici que q est impair. Écrire une fonction `factorisation_berlekamp_large` qui implante l'algorithme de Berlekamp dans le cas q grand (c'est-à-dire, en calculant $\mathrm{pgcd}(P, B)$, $\mathrm{pgcd}(P, B^{(q-1)/2} - 1)$ et $\mathrm{pgcd}(P, B^{(q-1)/2} + 1)$ où $B(X)$ correspond à un élément non-nul du noyau de ϕ. Retrouver expérimentalement la complexité en $O(n^3 + n^2 \log_2 q))$.

Question 5.– À l'aide de l'Exercice 3, prendre la Question 4 avec q pair.