Université Paris 8 Année 2022–2023

M2 Mathématiques et applications, parcours ACC

Algorithmes arithmétiques II – Solutions feuille de TD 4

13/10/2022

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. ($\star$) 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.

Solutions de l'Exercice 1.

Solution Q1. Si l'on note $\ell = dt$ avec $t \in \mathbb{Z}$, alors on a

$$q^\ell - 1 = q^{dt} - 1 = \left(q^d - 1\right)\left(1 + q^d + (q^d)^2 + \cdots + (q^d)^{t-1}\right)$$

Solution Q2. Notons $d = \deg P$. Alors $\mathbb{F}_q[X]/(P)$ est un corps de cardinal q^d. Donc la classe de X modulo P, notée α, vérifie

$$\alpha^{q^d - 1} = 1.$$

Supposons maintenant que $\ell \mid d$. D'après la question précédente, il existe $k \in \mathbb{Z}$ tel que $q^d - 1 = k(q^\ell - 1)$. Par conséquent, $\alpha^{q^\ell - 1} = \alpha^{k(q^d-1)} = 1^k = 1$. C'est-à-dire :

$$X^{q^\ell} \equiv X \mod P\,.$$

Solution Q3. Si $B(X) = \sum_{i=0}^m b_i X^i \in \mathbb{F}_q[X]$, alors on a :

$$B(X)^q = \sum_{i=0}^m b_i^q X^{iq} = \sum_{i=0}^m b_i X^{iq} \quad \text{car } b_i \in \mathbb{F}_q\,.$$

Cette relation s'étend naturellement aux puissances de q ; ainsi, $B(X)^{q^j} = \sum_{i=0}^m b_i X^{iq^j}$, pour tout $j \geq 1$. Comme dans la réponse à la question 2, on a toujours $X^{q^d} \equiv X \bmod P$ où $d = \deg P$. On obtient alors

$$B(X)^{q^d} = \sum_{i=0}^m b_i (X^{q^d})^i \equiv \sum_{i=0}^m b_i X^i \equiv B(X) \mod P\,.$$

Solution Q4. Supposons que $P(X)$ divise $X^{q^\ell} - X$. On vérifie alors (comme à la question précédente) que pour tout $B \in \mathbb{F}_q[X]$, on a $B(X)^{q^\ell} \equiv B(X) \mod P$. De plus, l'anneau $\mathbb{F}_q[X]/(P)$ est un corps et $B(X) \neq 0$, on a donc

$$B(X)^{q^\ell - 1} \equiv 1 \mod P$$

Pour $d = \deg P$, on écrit ensuite $\ell = du + r$ avec $u \in \mathbb{Z}$ et $0 \leq r < d$. Montrons que $r = 0$. On a d'abord

$$q^\ell - 1 = q^{du+r} - 1 = (q^{du} - 1)q^r + q^r - 1\,.$$

On sait également que $q^d - 1$ divise $q^{du} - 1$ d'après la question 1. Pour tout $B(X) \in \mathbb{F}_q[X]/(P)$, on a donc

$$1 \equiv B(X)^{q^\ell - 1} \equiv \underbrace{B(X)^{(q^{du}-1)q^r}}_{\equiv 1} B(X)^{q^r - 1} \equiv B(X)^{q^r - 1} \mod P\,.$$

Supposons $r \neq 0$. Alors, tout élément non-nul de $\mathbb{F}_q[X]/(P)$ est solution de l'équation $Y^{q^r - 1} - 1$ qui admet au plus $q^r - 1$ solutions. Comme $|\mathbb{F}_q[X]/(P) \setminus \{0\}| = q^d - 1 > q^r - 1$, c'est impossible. Donc $r = 0$.

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 d'un polynôme $Q(X)$, et calculer sa complexité en supposant $q \leq \deg(Q)$.

Solutions de l'Exercice 2.

Solution Q1. On a $P'(X) = q^2 X^{q^n - 1} - 1 = -1$ donc $\mathrm{pgcd}(P, P') = 1$. Le polynôme $P(X)$ ne contient donc aucun facteur carré.

Solution Q2. D'après le résultat de l'Exercice 1, les seuls polynômes irréductibles divisant $P(X)$ sont ceux dont le degré divise n. Par ailleurs, d'après la question précédente, la multiplicité de ces facteurs est au plus 1.

Solution Q3. ($\Rightarrow$) Si $Q(X)$ est irréductible, alors $Q(X)$ divise $X^{q^d} - X$, et pour tout $r \mid d$ tel que $r \neq d$, on ne peut pas avoir $Q(X) \mid X^{q^r} - X$ car sinon d diviserait r du fait du résultat de l'Exercice 1. Comme $Q(X)$ est irréductible, les polynômes $Q(X)$ et $X^{q^r} - X$ sont donc premiers entre eux.

($\Leftarrow$) Si $Q(X)$ divise $X^{q^d} - X$, et si pour tout $r \mid d$ tel que $r \neq d$, les polynômes $Q(X)$ et $X^{q^r} - X$ sont premiers entre eux, notons $U(X)$ un diviseur irréductible de $Q(X)$ de degré u. Alors, comme $U(X)$ divise $Q(X)$, $U(X)$ divise aussi $X^{q^d} - X$. Puis d'après l'Exercice 1, u divise d et par suite, $U(X)$ divise $X^{q^u} - X$ (car on suppose $U(X)$ irréductible). On en déduit que $U(X)$ divise le pgcd de $X^{q^u} - X$ et de $Q(X)$. Si $u \neq d$, on obtient alors une contradiction avec l'hypothèse initiale. Ainsi $u = d$, donc $U(X) = Q(X)$ à une unité près, donc $Q(X)$ est irréductible.

Solution Q4. L'algorithme est le suivant.

Entrée : un polynôme $Q(X) \in \mathbb{F}_q[X]$ de degré $d \geq 2$.
Sortie : `vrai` si le polynôme $Q(X)$ est irréductible ; `faux` sinon.

1. Pour tout r divisant d, $r \neq d$, faire :
   — Calculer efficacement $D(X) = \mathrm{pgcd}(X^{q^r} - X, Q)$.
   — Si $D(X) = 1$, retourner `faux`.
2. Retourner `vrai`

Il y a $O(d)$ calculs de pgcd à effectuer, à chaue fois entre deux polynômes dont les degrés peuvent être très différents : $q^r \in O(q^d)$ pour l'un, d pour l'autre. Chacun de ces pgcd consiste donc en une première division euclidienne « potentiellement coûteuse » (entre le polynôme $X^{q^r} - X$ et $Q(X)$ de degré d), puis $O(\log(d))$ divisions euclidiennes « peu coûteuses » (entre des polynômes de degré $O(d)$).

Observons maintenant que l'on peut calculer $X^{q^r} \mod Q$ plus efficacement qu'en faisant une division euclidienne : l'idée est de calculer successivement les puissances itérées $X^q \mod Q$, $(X^q)^q \mod Q$, ..., $X^{q^r} \mod Q$. Il y a donc $O(r)$ divisions euclidiennes à faire pour la partie « potentiellement coûteuse ».

Chaque division euclidienne ayant ensuite un coût en $O(d^2)$ opérations dans $\mathbb{F}_q$, on obtient un algorithme de complexité totale en $O(d^3 \log(d))$.

Remarque. Cette complexité peut être affinée si l'on a un algorithme de meilleure complexité pour la division euclidienne entre polynômes.

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 $\chi_i(F) := F \mod P_i \in \mathbb{F}_{2^k}[X]/(P_i)$.

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}.

Solutions de l'Exercice 3.

Solution Q1. Soit $A(X) \in \mathbb{F}_q[X]$. Alors,

$$T_m(A(X))^2 = (A(X)^{2^{m-1}} + A(X)^{2^{m-2}} + \cdots + A(X)^2 + A(X))^2 = A(X)^{2^m} + A(X)^{2^{m-1}} + \cdots + A(X)^4 + A(X)^2\,.$$

Donc

$$T_m(A(X))(T_m(A(X)) + 1) = T_m(A(X))^2 + T_m(A(X)) = A(X)^{2^m} + A(X)\,.$$

Solution Q2. Si $B(X) \in \mathbb{F}_{2^k}[X]$ vérifie $B(X)^{2^m} \equiv B(X) \mod P$, alors $B(X)^{2^m} + B(X) \equiv 0 \mod P$, donc $T_m(\alpha)^2 + T_m(\alpha) \equiv 0 \mod P$ d'après la question précédente. Aurtrement dit, $T_m(B(X))^2 \equiv T_m(B(X)) \mod P$.

Solution Q3. Soit $B(X) \in \mathcal{B}$. On rappelle que, par définition de l'algèbre de Berlekamp on a $B(X)^{2^k} \equiv B(X) \mod P$. D'après la question précédente, on a donc $T_k(B(X))^2 \equiv T_k(B(X)) \mod P$. Donc, en particulier, pour tout $i \in \{1, \ldots, r\}$, on a

$$T_k(B(X))^2 \equiv T_k(B(X)) \mod P_i\,.$$

Comme $\mathbb{F}_{2^k}[X]/(P_i)$ est une extension du corps fini $\mathbb{F}_{2^k}$, c'est en particulier une extension de $\mathbb{F}_2$. Les éléments laissés fixes par $z \mapsto z^2$ dans ce corps sont 0 et 1, donc $\chi_i(T_k(B(X))) \in \mathbb{F}_2$.

Cherchons maintenant à déterminer les $B(X) \in \mathcal{B}$ tels que $T_k(B) \in \mathbb{F}_2$. D'après le théorème des restes chinois, ce sont exactement ceux tels que pour tout i, on a $\chi_i \circ T_k(B) \in \{0,1\}$.

Notons que pour tout i, l'application $\chi_i \circ T_k : \mathcal{B} \to \mathbb{F}_2$ est $\mathbb{F}_2$-linéaire et non-nulle. Son noyau est donc de codimension 1. On a donc

$$\mathbb{P}((\chi_i \circ T_k)(B) = 0) = \frac{2^{\dim \ker \chi_i \circ T_k}}{2^{\dim \mathcal{B}}} = \frac{1}{2}.$$

Ainsi, on a également $\mathbb{P}((\chi_i \circ T_k)(B) = 1) = \frac{1}{2}$.

Par ailleurs, pour B une variable sur $\mathcal{B}$, les variables $\{\chi_i(T_k(B))\}$ sont indépendantes. Par conséquent,

$$\mathbb{P}(T_k(B) \in \{0,1\}) = \mathbb{P}(\forall i, (\chi_i \circ T_k)(B) = 0) + \mathbb{P}(\forall i, (\chi_i \circ T_k)(B) = 1) = 2 \times \frac{1}{2^r} = \frac{1}{2^{r-1}}$$

Remarque. L'algorithme de Berlekamp en grande cardinalité échoue quand $T_k(B) \in \mathbb{F}_2$. On a montré que cette probabilité est $\leq 1/2$.

Solution Q4. à venir

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.

Solutions de l'Exercice 4.

Voir scripts en documents annexes.

Les parties d'analyse de complexité des question 3 et 4, ainsi que la question 5, ne sont pas encore traitées (à venir).
