

Examen de M.A.O. Calcul Formel

Durée : 3 heures

Lorsqu'on évoque le coût d'un algorithme, on attend toujours une réponse de la forme $O(\dots)$: déterminer la constante implicite dans le symbole $O(\dots)$ n'est pas demandé. De plus, sauf mention explicite du contraire, on compte le nombre d'opérations arithmétiques (additions, multiplications, soustractions, divisions), dans $\mathbb{Z}$ ou dans un corps selon le contexte.

Les questions précédées du symbole $(\star)$ sont prévues pour être résolues, au moins en partie, à l'aide de **Sage**. Toutes les fonctions implémentées en **Sage** peuvent être utilisées, sauf mention explicite du contraire. Si une réponse est demandée dans la question, merci de la recopier sur la copie.

Il est autorisé d'admettre le résultat de certaines questions pour traiter les suivantes. L'exercice et le problème sont indépendants.

Exercice : intersection de deux courbes planes

Dans cet exercice on attend une preuve mathématique complète, rédigée en détails sur la copie à partir de résultats vus en cours, qui pourra s'appuyer sur des calculs faits en Sage.

$(\star)$ Déterminer les couples $(x, y) \in \mathbb{C}^2$ tels que

$$x^2 + y^2 = 1 \quad \text{et} \quad x^3 + x^2y + y^2 = 1.$$

Problème

Ce problème est constitué de 4 parties ; les deux premières sont indépendantes. La partie 3 (à partir de la question 15) et la partie 4 utilisent la partie 1, et aussi éventuellement (pour des questions de **Sage**) la partie 2.

Partie 1 : Suites périodiques dans $\mathbb{F}_p^d$

Dans cette partie on fixe un nombre premier p , un entier $d \geq 1$, et une matrice inversible $N \in \text{GL}_d(\mathbb{F}_p)$. Etant donné une matrice colonne $U \in \text{M}_{d,1}(\mathbb{F}_p) \setminus \{0\}$ on considère la suite $(U_j)_{j \geq 0}$ définie par $U_j = N^j U$ pour tout $j \in \mathbb{N}$.

1. Montrer que la suite (U_j) est périodique, et que sa période (notée $T_{N,U}$) divise l'ordre de N dans le groupe $\text{GL}_d(\mathbb{F}_p)$.
2. Démontrer que $T_{N,U}$ est le plus petit entier $j \geq 1$ tel que $N^j U = U$.
3. $(\star)$ Dans cette question seulement on pose $p = 31$, $d = 3$, et on considère la matrice

$$N = \begin{bmatrix} 2 & 5 & 7 \\ 3 & 1 & 17 \\ 1 & 4 & 12 \end{bmatrix} \in \text{GL}_d(\mathbb{F}_p).$$

Calculer $T_{N,U}$ pour chacun des choix suivants de U : $\begin{bmatrix} 1 \\ 19 \\ 30 \end{bmatrix}$, $\begin{bmatrix} 2 \\ 1 \\ 17 \end{bmatrix}$.

4. Déterminer le coût, en nombre d'opérations arithmétiques dans $\mathbb{F}_p$, du calcul de $T_{N,U}$; on exprimera ce coût en fonction de d et de $T_{N,U}$ lui-même, puis le majorer en fonction de d et p seulement.
5. Fixons $N \in \text{GL}_d(\mathbb{F}_p)$. Montrer que si $T_{N,U} = p^d - 1$ pour un certain $U \in \text{M}_{d,1}(\mathbb{F}_p) \setminus \{0\}$, alors $T_{N,U} = p^d - 1$ pour tout $U \in \text{M}_{d,1}(\mathbb{F}_p) \setminus \{0\}$.
6. En quelques mots, à quoi pourrait servir une telle suite lorsque $T_{N,U} = p^d - 1$?

Partie 2 : Générateurs de $\mathbb{K}^\times$ pour un corps fini $\mathbb{K}$

Dans cette partie on fixe un corps fini $\mathbb{K}$ dont on note q le cardinal. On suppose connue la décomposition en facteurs premiers de $q - 1$, notée

$$q - 1 = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}$$

avec $p_1 < \dots < p_r$ premiers et $\alpha_1, \dots, \alpha_r \geq 1$.

7. Soit $g \in \mathbb{K}^\times$. Montrer que g est un générateur du groupe multiplicatif $\mathbb{K}^\times$ si, et seulement si, $g^{(q-1)/p_i} \neq 1$ pour tout $i \in \llbracket 1, r \rrbracket$.
8. (★) Implémenter en **Sage** une fonction `est_generateur` qui prend en entrée un corps fini $\mathbb{K}$, un élément $g \in \mathbb{K}^\times$ et la liste des facteurs premiers de $q - 1$, et renvoie `True` si g est un générateur de $\mathbb{K}^\times$ et `False` sinon.
9. (★) Dans cette question on prend $q = 17^2$ et on implémente le corps $\mathbb{K}$ comme étant $\mathbb{F}_{17}[X]/(P)$, avec $P(X) = X^2 + X + 1$. On note $x \in \mathbb{K}$ la classe de X . En utilisant la fonction `est_generateur`, déterminer si chacun des trois éléments suivants est un générateur de $\mathbb{K}^\times$ ou pas :

$$g_1 = x + 5, \quad g_2 = 3x, \quad g_3 = 15x + 11.$$

10. Déterminer le coût de la fonction `est_generateur` de la question 8, en nombre d'opérations arithmétiques dans $\mathbb{K}$, d'abord en fonction de q et du nombre r de facteurs premiers de $q - 1$, puis en fonction de q seulement.
11. (★) En utilisant la fonction `est_generateur` de la question 8 et la méthode `K.random_element()` qui renvoie un élément aléatoire de $\mathbb{K}$ (pour la loi uniforme), implémenter en **Sage** une fonction `calcul_generateur` qui prend en entrée un corps fini $\mathbb{K}$ et la liste des facteurs premiers de $q - 1$, et renvoie un générateur de $\mathbb{K}^\times$.
12. (★) Déterminer un générateur de $\mathbb{K} = \mathbb{F}_3[X]/(P)$, avec $P(X) = X^2 + 1$, en utilisant la fonction `calcul_generateur`.
13. Dans cette question seulement, on suppose que $q - 1$ est une puissance de 2. Déterminer, en moyenne, le coût en nombre d'opérations arithmétiques dans $\mathbb{K}$ de la fonction `calcul_generateur` de la question 11.

Partie 3 : Multiplication par un générateur

Dans cette partie on fixe un corps fini $\mathbb{K}$ dont on note q le cardinal. On note p la caractéristique de $\mathbb{K}$ et $d \geq 1$ l'entier tel que $q = p^d$. On suppose connu un polynôme irréductible unitaire $P \in \mathbb{F}_p[X]$ de degré d , et on identifie $\mathbb{K}$ à $\mathbb{F}_p[X]/(P)$. On note x l'image de X dans ce quotient, et on identifie un élément y de $\mathbb{K}$ à l'unique d -uplet $(a_0, \dots, a_{d-1}) \in \mathbb{F}_p^d$ tel que $y = \sum_{i=0}^{d-1} a_i x^i$.

14. Rappeler brièvement comment on implémente les quatre opérations (addition, soustraction, multiplication, division) dans $\mathbb{K}$, et quel est le coût de chacune d'entre elles en nombre d'opérations arithmétiques dans $\mathbb{F}_p$.

Dans la suite on suppose connu un générateur g de $\mathbb{K}^\times$ et on note $\mu : \mathbb{K} \rightarrow \mathbb{K}$ la multiplication par g , définie par $\mu(y) = gy$ pour tout $y \in \mathbb{K}$. On note M la matrice de l'application $\mathbb{F}_p$ -linéaire μ dans la base $(1, x, \dots, x^{d-1})$.

15. Soit $U \in M_{d,1}(\mathbb{F}_p) \setminus \{0\}$ une matrice colonne non nulle de taille d . Avec les notations de la question 1, démontrer que $T_{M,U} = p^d - 1$.

16. Notons Q le polynôme minimal de g sur $\mathbb{F}_p$. Montrer que Q est unitaire de degré d .

On note $N \in M_d(\mathbb{F}_p)$ la matrice compagnon du polynôme Q défini à la question 16. On rappelle qu'en notant $Q(X) = X^d + \sum_{i=0}^{d-1} q_i X^i$, et en indexant les coefficients $n_{i,j}$ de N par $i, j \in \llbracket 0, d-1 \rrbracket$, on a :

$$n_{i,j} = \begin{cases} 1 & \text{si } i = j + 1 \text{ et } 0 \leq j \leq d-2, \\ -q_i & \text{si } j = d-1, \\ 0 & \text{sinon.} \end{cases}$$

Si $d = 1$, on convient que l'unique coefficient de N est $-q_0$.

17. Montrer que M et N sont semblables dans $M_d(\mathbb{F}_p)$.
 18. En déduire que la conclusion de la question 15 est vraie en remplaçant M par N .
 19. Montrer que N est inversible et calculer son ordre dans le groupe $\text{GL}_d(\mathbb{F}_p)$.

Partie 4 : Matrices compagnons

Dans cette partie on considère un nombre premier p et un polynôme $Q \in \mathbb{F}_p[X]$ unitaire, irréductible, de degré $d \geq 1$; on suppose aussi $Q \neq X$. On note N la matrice compagnon associée à Q , dont la définition est rappelée juste avant la question 17. On pourra utiliser sans démonstration la propriété bien connue suivante : le polynôme caractéristique de N et son polynôme minimal sont tous les deux égaux à Q .

20. Montrer que N est inversible et que son ordre dans le groupe $\text{GL}_d(\mathbb{F}_p)$ divise $p^d - 1$.
 21. Dans le cas $d = 1$, montrer que pour tout diviseur δ de $p^d - 1$ il existe Q tel que l'ordre de la matrice N associée soit égal à δ .
 22. Montrer que l'ordre de N dans $\text{GL}_d(\mathbb{F}_p)$ est égal à l'ordre de la classe de X dans le groupe multiplicatif $\mathbb{K}^\times$, où $\mathbb{K} = \mathbb{F}_p[X]/(Q)$.
 23. (★) Dans cette question on prend $p = 11$ et $d = 2$. Exhiber un polynôme irréductible unitaire $Q \in \mathbb{F}_p[X]$ de degré d tel que la matrice N associée ne soit pas d'ordre $p^d - 1$ dans $\text{GL}_d(\mathbb{F}_p)$.
 24. Avec les notations de la question 1, démontrer que N est d'ordre $p^d - 1$ dans $\text{GL}_d(\mathbb{F}_p)$ si, et seulement si, on a $T_{N,U} = p^d - 1$ pour tout $U \in M_{d,1}(\mathbb{F}_p) \setminus \{0\}$.
 25. (★) Dans cette question on pose $p = 7$ et $d = 3$. On note $\mathcal{A}$ l'ensemble des $Q \in \mathbb{F}_p[X]$ unitaires, irréductibles, de degré 3, tels que la matrice N associée soit d'ordre $p^d - 1$ dans $\text{GL}_d(\mathbb{F}_p)$. Répondre aux questions suivantes en énumérant les éléments de $\mathcal{A}$:
 (a) Combien y a-t-il d'éléments dans $\mathcal{A}$?
 (b) Combien vaut le produit (noté P) des éléments de $\mathcal{A}$?
 26. (★) (Bonus) Essayer de reconnaître le polynôme P de la question 25 (b), et vérifier votre observation sur d'autres couples (p, d) .