

Partiel de M.A.O. Calcul Formel Durée : 3 heures

Vendredi 21 avril 2017
Master 1 M.F.A., Orsay

L'accès à internet et l'utilisation des téléphones portables sont interdits. Les documents et notes de cours sont interdits, à l'exception du livre "Calcul mathématique avec Sage". En revanche l'aide de Sage et une version pdf de ce livre sont disponibles sur les ordinateurs. Ce partiel est une épreuve de mathématiques. Avant d'utiliser l'ordinateur, il convient de se demander s'il n'est pas possible d'obtenir par un raisonnement simple ce qui pourrait être obtenu par un calcul plus complexe fait par ordinateur. A titre indicatif, dans les questions signalées par le signe ($\star$), on s'attend à une réponse utilisant de façon essentielle l'ordinateur ; pour les autres, on s'attend davantage à une réponse argumentée, utilisant éventuellement l'ordinateur mais de façon plus marginale.
Dans tous les cas, si vous utilisez l'ordinateur, vous devez recopier les lignes de code Sage que vous avez utilisées (en faisant attention à l'indentation), et ce que leur exécution a renvoyé ; il est également indispensable d'expliquer les calculs que vous faites faire à l'ordinateur. Il est parfois indiqué que certaines commandes de Sage ne doivent pas être utilisées ; en cas de doute n'hésitez pas à poser des questions pendant l'épreuve.

Le sujet est composé d'un seul problème, découpé en trois parties. Il est possible d'admettre le résultat de certaines questions pour traiter les suivantes. Dans l'ensemble, les premières questions de chaque partie sont plutôt plus faciles que les dernières.

Dans tout le problème, $\mathbb{K}$ désigne un corps fixé.

Partie 1 : Un algorithme bien connu.

Dans cette première partie, on fixe deux polynômes $A, B \in \mathbb{K}[X]$ tels que $\deg A > \deg B > 0$. On définit par récurrence des polynômes U_j, V_j, R_j comme suit. On pose $R_0 = A$, $R_1 = B$, $U_0 = 1$, $U_1 = 0$, $V_0 = 0$, $V_1 = 1$. Pour tout $j \geq 2$ tel que $R_{j-1} \neq 0$, on note Q_{j-2} le quotient et R_j le reste dans la division euclidienne de R_{j-2} par R_{j-1}, et on pose $U_j = U_{j-2} - Q_{j-2}U_{j-1}$ et $V_j = V_{j-2} - Q_{j-2}V_{j-1}$. Comme on l'a vu en cours, il existe un entier $\ell \geq 2$ tel que $R_\ell = 0$; les polynômes U_j, V_j, R_j sont définis pour $0 \leq j \leq \ell$ et Q_j pour $0 \leq j \leq \ell - 2$. On rappelle aussi les propriétés suivantes, qu'on pourra utiliser sans démonstration :

$$\deg U_{j+2} = \deg B - \deg R_{j+1} \text{ et } \deg V_{j+2} = \deg A - \deg R_{j+1} \text{ pour } 0 \leq j \leq \ell - 2;$$

$$R_j = AU_j + BV_j \text{ pour } 0 \leq j \leq \ell.$$

1. Rappeler le nom de cet algorithme, ce que fournit $(R_{\ell-1}, U_{\ell-1}, V_{\ell-1})$, et le coût de ce calcul en opérations arithmétiques (additions, multiplications, divisions dans $\mathbb{K}$). *Dans cette question, aucune justification n'est demandée.*

2. Rappeler *sans démonstration* le coût en opérations arithmétiques (additions, multiplications, divisions dans $\mathbb{K}$) de la division euclidienne de A par B.

3. ($\star$) Tout au long de ce problème nous allons considérer, parallèlement au cas général, l'exemple des polynômes

$$A_0 = X^8 \quad \text{et} \quad B_0 = X^7 - X^5 + X^3 - X, \quad \text{avec } \mathbb{K} = \mathbb{Q}.$$

Appliquer l'algorithme ci-dessus avec A_0 et B_0 : déterminer ℓ ainsi que R_j, U_j et V_j pour tout $j \in \{2, \dots, \ell\}$. *On s'interdira, ici et dans tout ce problème, d'utiliser la fonction de Sage qui implémente directement l'algorithme en question ; on utilisera en revanche les commandes* `q` = p//d *et* `r` = p % d *pour calculer le quotient q et le reste r dans la division euclidienne de p par d, ou alors de façon équivalente la commande* `q,r` = p.quo_rem(d).

4. Soit $j \in \{0, \dots, \ell - 2\}$. Exhiber une matrice M_j à coefficients dans $\mathbb{K}[X]$, de déterminant -1, telle que

$$\begin{bmatrix} U_{j+1} & V_{j+1} \\ U_{j+2} & V_{j+2} \end{bmatrix} = M_j \cdot \begin{bmatrix} U_j & V_j \\ U_{j+1} & V_{j+1} \end{bmatrix}.$$

5. Déduire de la question précédente que pour tout $j \in \{0, \dots, \ell\}$ on a $\operatorname{pgcd}(U_j, V_j) = 1$.

6. Dans cette question on se donne trois polynômes $R, U, V \in \mathbb{K}[X]$ tels que

$$V \neq 0, \quad R = AU + BV \quad \text{et} \quad \deg R + \deg V < \deg A.$$

   (*a*) Justifier qu'il existe un entier $r \in \{1, \dots, \ell\}$, et un seul, vérifiant l'encadrement $\deg R_r \leq \deg R < \deg R_{r-1}$.

   (*b*) Démontrer qu'on a $\deg(R_r V - R V_r) < \deg A$.

   (*c*) Démontrer que $R_r V - R V_r = A(U_r V - U V_r)$, puis en déduire (en utilisant la question précédente) que $U_r V = U V_r$.

   (*d*) Démontrer qu'il existe un polynôme $S \in \mathbb{K}[X]$ tel que $U = SU_r$, $V = SV_r$ et $R = SR_r$.

Partie 2 : Etude d'un ensemble $\mathcal{E}(A, k)$.

Dans la suite on fixe un entier $N \geq 1$ et un polynôme $B(X) = \sum_{i=0}^{N-1} b_i X^i \in \mathbb{K}[X]$ de degré $< N$. Etant donnés un polynôme $A \in \mathbb{K}[X]$ de degré $\geq N$ et un entier $k \in \{1, \dots, \deg A\}$, on note $\mathcal{E}(A, k)$ l'ensemble des couples $(R, V) \in \mathbb{K}[X]^2$ tels que

$$BV \equiv R \bmod A, \quad \deg R < k \quad \text{et} \quad \deg V \leq \deg A - k.$$

On garde les notations de la première partie (relatives aux mêmes polynômes A et B), et on note t le plus petit entier tel que $\deg R_t < k$.

7. Démontrer que $(R_t, V_t) \in \mathcal{E}(A, k)$.

8. ($\star$) En reprenant les notations et les calculs de la question 3 et en utilisant la question précédente, déterminer un élément de $\mathcal{E}(A_0, 4)$ lorsque $B = B_0$ et $N = 8$.

9. Soit (R, V) un élément de $\mathcal{E}(A, k)$: il existe $U \in \mathbb{K}[X]$ tel que $R = AU + BV$. On suppose $V \neq 0$, et on note r l'entier donné par la question 6(a) de la première partie.

   (a) Démontrer qu'on a $r \geq t$.

   (b) Démontrer que $r = t$ et qu'il existe un polynôme $S \in \mathbb{K}[X]$ tel que $R = SR_r$ et $V = SV_r$. *Indication : on pourra appliquer deux fois la question 6.*

Partie 3 : Application aux récurrences linéaires.

On fixe un entier $N \geq 1$ et une suite $(b_0, \ldots, b_{N-1})$ d'éléments de $\mathbb{K}$.

Comme dans la partie précédente, on note $B(X) = \sum_{i=0}^{N-1} b_i X^i$ le polynôme de degré $< N$ de $\mathbb{K}[X]$ ayant ces b_i comme coefficients.

Plus généralement, on reprend les notations des parties précédentes.

On dit que la suite $(b_0, \ldots, b_{N-1})$ vérifie une relation de récurrence linéaire d'ordre $\leq m$ si il existe $v_0, \ldots, v_m \in \mathbb{K}$ tels que

$$v_m b_i + v_{m-1} b_{i+1} + \ldots + v_0 b_{i+m} = 0 \text{ pour tout } i \in \{0, \ldots, N-1-m\}. \qquad (1)$$

10. Démontrer que si $m \geq N/2$ alors toute suite $(b_0, \ldots, b_{N-1})$ vérifie une relation de récurrence linéaire d'ordre $\leq m$ non triviale (c'est-à-dire telle que $(v_0, \ldots, v_m) \neq (0, \ldots, 0)$). *Indication : considérer qu'il s'agit d'un problème d'algèbre linéaire.*

11. Supposons N pair et posons $m = N/2$. Comment peut-on relier les $(m+1)$-uplets $(v_0, \ldots, v_m) \in \mathbb{K}^{m+1}$ vérifiant (1) aux éléments de $\mathcal{E}(X^N, m)$? Expliquer alors comment déduire des parties précédentes un algorithme qui calcule une relation de récurrence linéaire d'ordre $\leq m$ non triviale. Quel est le coût de cet algorithme en opérations arithmétiques (additions, multiplications, divisions dans $\mathbb{K}$) ?

12. ($\star$) Dans le cas de la suite $(b_0, \ldots, b_7) = (0, -1, 0, 1, 0, -1, 0, 1)$, déterminer la relation de récurrence linéaire d'ordre ≤ 4 obtenue à partir des calculs effectués à la question 8.

13. ($\star$) Déterminer une relation de récurrence linéaire non triviale d'ordre ≤ 5 vérifiée par la suite $(b_0, \ldots, b_9) = (3, 1, 4, 1, 5, 9, 2, 6, 5, 3)$ formée par les 10 premières décimales de π. *Les nombres calculés par Sage augmentant assez vite, on écrira sur la copie les calculs demandés à Sage mais pas les réponses fournies ; on notera simplement sur la copie les valeurs de v_0 et de v_1 obtenues.*

14. ($\star$) La suite des 200 premières décimales de π vérifie-t-elle une relation de récurrence linéaire non triviale d'ordre ≤ 80 ? *On rappelle qu'en Sage, le nombre π est accessible par l'instruction* `pi`