UFR de Mathématiques et Informatique
Université Bordeaux I

Année 1999–2000

Licence de Mathématiques et Informatique

Module d'Algorithmique Arithmétique

Session de septembre 2000

Durée 3 heures

Documents interdits. Le barème (donné sur 20 points) n'est qu'indicatif.

Exercice I (9 points)

Pour deux polynômes P et Q de $\mathbb{R}[X]$, on pose

$$< P, Q >= \int_0^1 \frac{P(x)Q(x)}{\sqrt{x}}\, dx \; .$$

1) a) Expliquer brièvement pourquoi l'intégrale est convergente.

b) Démontrer que $< P, Q >$ définit un produit scalaire sur $\mathbb{R}[X]$ (on prendra bien soin de démontrer ceci rigoureusement).

On notera $P_n(X)$ la famille de polynômes orthogonaux pour ce produit scalaire (avec $\deg(P_n) = n$) normalisés en demandant que les P_n soient unitaires.

2) En appliquant le procédé d'orthogonalisation de Gram–Schmidt à la famille $(1, X, X^2)$, calculer explicitement $P_0(X)$, $P_1(X)$ et $P_2(X)$.

3) On pose

$$Q_n(X) = \sqrt{X}\frac{d^n}{dX^n}\left(X^{n-\frac{1}{2}}(X-1)^n\right) \; .$$

a) Montrer que $Q_n(X)$ est un polynôme en X, de degré égal à n.

b) Par des intégrations par parties successives, montrer que pour tout polynôme $A(X)$ de degré au plus égal à $n-1$, on a $< Q_n, A >= 0$.

c) En déduire qu'il existe une famille de constantes c_n telles que $P_n(X) = c_n Q_n(X)$, où $P_n(X)$ sont les polynômes orthogonaux normalisés comme ci-dessus.

d) Calculer la constante c_n en calculant explicitement le coefficient dominant de Q_n. Exprimer le résultat à l'aide de factorielles. On rappelle le résultat suivant (qu'il est inutile de redémontrer)

$$1 \cdot 3 \cdot 5 \cdots (2k-1) = \frac{(2k)!}{2^k k!} \; .$$

4) On rappelle que toute famille de polynômes orthogonaux, et en particulier la famille $P_n(X)$, vérifie une récurrence du type

$$P_{n+1}(X) = (u_n X + v_n) P_n(X) + w_n P_{n-1}(X)$$

pour certaines suites u_n, v_n et w_n.

a) Expliquer (en une ligne) pourquoi $u_n = 1$.

b) En développant $(X-1)^n$ par la formule du binôme, calculer explicitement tous les coefficients du polynôme $Q_n(X)$, puis les coefficients du polynôme $P_n(X)$.

c) Ecrivons $P_n(X) = X^n + a_n X^{n-1} + b_n X^{n-2} + \cdots$. En identifiant les coefficients de X^n et de X^{n-1}, exprimer v_n et w_n en fonction de a_n et b_n.

d) En déduire les valeurs explicites de v_n et w_n.

Exercice II (4 points)

1) Démontrer que la norme d'une matrice est égale à sa plus grande valeur singulière.

2) On pose

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 5 & 5 & 5 \\ 7 & 7 & 7 \end{pmatrix} .$$

a) Trouver une décomposition en valeur singulière (SVD) de A sous la forme $A = UDV^t$ avec U et V orthogonale et D diagonale.

b) Déduire de la première question la norme de A.

3) Calculer le pseudoinverse $A^\dagger$ de A.

Exercice III (7 points)

Soit K un corps commutatif. Pour a et b dans K on pose

$$M(a,b) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} ,$$

et on note A l'ensemble de toutes les matrices $M(a,b)$ quand a et b parcourent K.

1) a) Montrer que A est un sous-anneau de l'anneau des matrices 2×2 à coefficients dans K.

b) Montrer que A est commutatif.

2) a) Soit $M = M(a,b)$ un élément de A. Exprimer M^2 comme combinaison linéaire de M et de I, matrice identité d'ordre 2 (y-a-t'il une manière d'obtenir ce résultat sans calcul ?).

b) En déduire pour tout entier $n \geq 1$ une expression de M^{n+1} en fonction de M^n et M^{n-1}.

c) D'après 1a), on peut écrire

$$M^n = \begin{pmatrix} u_n & -v_n \\ v_n & u_n \end{pmatrix}$$

pour certaines suites u_n et v_n d'éléments de K. Montrer que u_n et v_n satisfont à la même récurrence

$$x_{n+1} = 2ax_n - (a^2 + b^2)x_{n-1} \ ,$$

et préciser les valeurs initiales u_0, u_1, v_0 et v_1.

3) On suppose désormais que p est un nombre premier tel que $p \equiv 3 \pmod 4$, et que $K = \mathbb{F}_p$ (identifié à $\mathbb{Z}/p\mathbb{Z}$) est le corps à p éléments. On pose

$$J = M(0,1) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \ ,$$

de sorte que $M(a,b) = aI + bJ$.

a) Calculer J^2.

b) En utilisant la représentation $M(a,b) = aI + bJ$, montrer que $M(a,b)^p = aI - bJ$. Cette question étant l'une des plus importantes de cet exercice, il est demandé de la résoudre avec soin.

c) En déduire $M(a,b)^{p+1}$. Que vaut v_{p+1} ?

4) Soient α et β deux entiers. On considère la suite d'entiers z_n définie par $z_{n+1} = 2\alpha z_n - (\alpha^2 + \beta^2)z_{n-1}$ avec les conditions initiales $z_0 = 0$, $z_1 = \beta$.

a) Soit a (resp. b) la classe de α (resp. β) dans $\mathbb{Z}/p\mathbb{Z}$. Avec les notations des questions précédentes, montrer que la classe modulo p de z_n est égale à v_n.

b) Déduire de ceci et de la question 3c) que $z_{p+1} \equiv 0 \pmod p$ (ceci est un analogue du petit théorème de Fermat).

5) Application numérique : on pose $p = 23$, et on considère la suite de Fibonacci définie par la récurrence $F_{n+1} = F_n + F_{n-1}$ avec les conditions initiales $F_0 = 0$ et $F_1 = 1$. Déduire de la question 4b) que $F_{24} \equiv 0 \pmod{23}$ (on choisira $\alpha = 12$ et $\beta = 4$, et on montrera que la suite d'entiers z_n correspondante vérifie $z_n \equiv 4F_n \pmod{23}$).