UFR de Mathématiques et Informatique
Université Bordeaux I — Année 2001–2002

Licence de Mathématiques et Informatique

Module d'Algorithmique Arithmétique

Examen du 21 janvier 2002

Durée 3 heures

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

Exercice I (8 points)

Soit $A(X) \in \mathbb{R}[X]$ un polynôme fixé non identiquement nul et tel que $A(x) \geq 0$ pour $x \in [-1, 1]$. Pour deux polynômes P et Q de $\mathbb{R}[X]$, on pose

$$< P, Q >= \int_{-1}^{1} P(x)Q(x)A(x)\, dx \ .$$

1) Montrer *soigneusement* mais brièvement que $< P, Q >$ définit un produit scalaire sur $\mathbb{R}[X]$. On note $P_n(X)$ la famille de polynômes orthogonaux pour ce produit scalaire (avec $\deg(P_n) = n$) normalisés en demandant que les P_n soient unitaires.

2) On cherche les polynômes $A(X)$ pour lesquels on ait

$$P_n(X) = \frac{c_n}{A(X)} \frac{d^n}{dX^n}(A(X)(1 - X^2)^n) \ ,$$

où c_n est une constante non nulle convenable.

a) Calculer $P_1(X)$ en fonction de c_1 et de $A(X)$. En utilisant le fait que $P_1(X)$ doit être un polynôme de degré 1, montrer que les seules racines de $A(X)$ dans $\mathbb{C}$ sont -1 et 1. En déduire que $A(X)$ est de la forme $A(X) = c(1 - X)^a(1 + X)^b$ pour des entiers positifs ou nuls a et b et une constante réelle strictement positive c.

b) Réciproquement, si $A(X)$ est de la forme ci-dessus, montrer qu'il existe des constantes c_n convenables telles que les polynômes

$$P_n(X) = \frac{c_n}{A(X)} \frac{d^n}{dX^n}(A(X)(1 - X^2)^n)$$

forment l'unique famille de polynômes orthogonaux unitaires pour le produit scalaire $< P, Q >$ (on n'oubliera pas de montrer que les $P_n(X)$ sont bien des polynômes).

c) Calculer la constante c_n en fonction de a et de b.

3) On pose

$$P_n(X) = X^n + \lambda_n X^{n-1} + \mu_n X^{n-2} + \dots$$

et on rappelle que la famille P_n vérifie une équation de récurrence du type

$$P_n(X) = (X + a_n)P_{n-1}(X) + b_n P_{n-2}(X)$$

pour des a_n et b_n convenables.

En identifiant les coefficients de X^{n-1} et X^{n-2} dans l'équation de récurrence, calculer a_n et b_n en fonction de λ_n et μ_n.

A partir de maintenant, on étudie le cas particulier $a = 2$, $b = 1$, c'est à dire $A(X) = (1 - X)^2(1 + X)$. On rappelle la formule (qu'il est inutile de démontrer) : pour $m \geq n$ on a

$$\frac{d^n}{dX^n} X^m = \frac{m!}{(m-n)!} X^{m-n} \quad .$$

a) Calculer explicitement λ_n et μ_n (on remarquera que $2n + 2 = 2(n + 1)$).

b) Déduire de la question 3) les valeurs de a_n et b_n, et donc la formule de récurrence pour les P_n.

Exercice II (8 points)

On pose $A = \{\alpha = u + iv, \ u, v \in \mathbb{Z}\}$ et $K = \{\alpha = u + iv, \ u, v \in \mathbb{Q}\}$.

1) a) Montrer brièvement que K est un corps et que A est un sous-anneau de K. En particulier, si α et β appartiennent à A avec $\beta \neq 0$ on a $\alpha/\beta \in K$.

b) Pour tout $\alpha = u + iv \in K$, on pose

$$\phi(\alpha) = \alpha\overline{\alpha} = u^2 + v^2 \ .$$

Montrer que ϕ est un stathme euclidien sur A (si $\alpha/\beta = u + iv$ avec u, $v \in \mathbb{Q}$ on pourra poser $q = \lfloor u \rceil + i\lfloor v \rceil$, où $\lfloor x \rceil$ désigne l'entier le plus proche de x).

Il en résulte que A est un anneau euclidien, donc principal.

2) On considère l'idéal $I = 4A$. Déterminer un ensemble E ayant exactement quatre éléments tel que si $\alpha \in A$, alors il existe $\beta \in E$ tel que $\alpha^2 \equiv \beta \pmod I$ (en d'autres termes $\alpha^2 - \beta \in I$).

3) On cherche à trouver la solution générale de l'équation $\alpha^2 + \beta^2 + \gamma^2 = 0$ avec α, β et γ dans A. On pose $\delta = (\alpha, \beta)$, un PGCD de α et β.

a) Montrer que δ divise γ. En déduire que si on pose $a = \alpha/\delta$, $b = \beta/\delta$ et $c = \gamma/\delta$ on a $a^2 + b^2 + c^2 = 0$ avec a, b et c appartenant à A et premiers entre eux deux à deux

On étudie donc désormais cette équation avec cette dernière hypothèse.

b) En utilisant la question 2), montrer que a, b ou c appartient à $2A$, et exactement un seul d'entre eux appartient à $2A$. Quitte à permuter a, b et c, on peut supposer que $c \in 2A$.

c) On pose $x = (a+ib)/2$ (attention, a et b sont dans A donc ne sont en général pas la partie réelle et imaginaire de $2x$). Montrer que notre équation peut s'écrire sous la forme $x(x-a) = (c/2)^2$

d) On rappelle que $c/2 \in A$. Déduire de c) que $x \in A$ (on écrira $x = \alpha/\beta$ avec α et β dans A premiers entre eux, et on montrera que β est inversible dans A).

e) Montrer que x et $x-a$ sont premiers entre eux (on montrera qu'un diviseur commun divise a, puis $b = (a-2x)i$).

f) En utilisant par exemple l'existence de la décomposition en facteurs premiers dans A, en déduire qu'il existe s et t dans A tels que, ou bien $x = s^2$ et $x - a = t^2$, ou bien $x = is^2$ et $x - a = it^2$.

g) En déduire la solution générale dans A de l'équation $\alpha^2 + \beta^2 + \gamma^2 = 0$.

Exercice III (4 points)

Soient a, b et c trois nombres réels non tous trois nuls, et soit A la matrice

$$A = \begin{pmatrix} a & a & a \\ b & b & b \\ c & c & c \end{pmatrix} .$$

On pose $N = a^2 + b^2 + c^2$.

1) Trouver une décomposition en valeur singulière (SVD) de A sous la forme $A = UDV^t$ avec U et V orthogonales et D diagonale (on suggère de calculer d'abord les matrices D et V).

2) a) Calculer le pseudoinverse $A^\dagger$ de A en utilisant la SVD trouvée ci-dessus.

b) Retrouver ce résultat en utilisant la caractérisation de $A^\dagger$ comme l'unique matrice telle que $AA^\dagger$ et $A^\dagger A$ soient des matrices symétriques, et que $AA^\dagger A = A$ et $A^\dagger AA^\dagger = A^\dagger$. Pour cela, on montrera que $A^\dagger = \lambda A^t$ satisfait ces conditions pour une valeur convenable de λ.

Exercice IV (0 point)

Cet exercice ne devra *pas* être traité pendant l'examen, et est simplement donné comme suite intéressante de l'Exercice II.

On cherche à trouver tous les cubes de $\mathbb{R}^3$ dont les sommets se projettent sur le plan $z = 0$ en des points à coordonnées entières. Quitte à faire une translation, on peut supposer que l'un des sommets est à l'origine $(0,0,0)^t$. Soient $P_i = (x_i, y_i, z_i)^t$ pour $i = 1$, 2 et 3 les trois sommets adjacents au sommet origine. Le point P_i se projette donc sur le point $Q_i = (x_i, y_i)$ dans le plan $z = 0$.

1) Donner les coordonnées des 8 sommets du cube. En déduire que ses sommets se projettent en des points à coordonnées entières si et seulement si les Q_i sont à coordonnées entières.

2) On appelle m le coté du cube.

a) Soit A la matrice 3×3 dont les colonnes sont les coordonnées des P_i pour $i = 1$, 2 et 3. Montrer que $A^t A = m^2 I$, où I est la matrice identité d'ordre 3, et réciproquement que si ceci est vérifié les colonnes de A sont les coordonnées des sommets d'un cube de coté m.

b) En déduire que $AA^t = m^2 I$ (bien que facile, c'est le cœur de cet exercice et de la magie noire).

c) En déduire les relations

$$x_1^2 + x_2^2 + x_3^2 = y_1^2 + y_2^2 + y_3^2$$
$$x_1 y_1 + x_2 y_2 + x_3 y_3 = 0 \ .$$

d) Réciproquement, montrer que si ces relations sont vérifiées il existe z_1, z_2, z_3 tels que les points P_i correspondants forment bien les sommets adjacents à l'origine d'un cube.

3) a) On pose $\alpha = x_1 + iy_1$, $\beta = x_2 + iy_2$ et $\gamma = x_3 + iy_3$. Montrer que les deux équations du 2c) sont équivalentes à l'unique équation $\alpha^2 + \beta^2 + \gamma^2 = 0$ dans l'anneau A de l'Exercice II.

b) Déduire de l'Exercice II la solution générale du problème posé ici.

c) Application numérique : trouver des exemples de cubes qui se projettent en 8 points distincts et à coordonnées entières du plan $z = 0$. Faire les dessins correspondants.

Remarque. Les Exercices II et IV forment une partie d'un problème posé à l'écrit du CAPES de Mathématiques.