UFR de Mathématiques et Informatique
Université Bordeaux I

Année 1999–2000

Licence de Mathématiques et Informatique

Module d'Algorithmique Arithmétique

Corrigé de la session de septembre 2000

Exercice I

1) a) Le seul problème est en 0. Or nous savons que l'intégrale de $1/x^a$ est convergente au voisinage de 0 si et seulement si $a < 1$, donc puisqu'ici $a = 1/2$, l'intégrale converge.

b) Il est clair que $< P, Q >$ est une forme bilinéaire, que $< P, P > \geq 0$, et que $< 0, 0 >= 0$. Il faut montrer que $< P, P >= 0$ implique que $P = 0$. Comme d'habitude, ceci résulte du fait que si l'intégrale d'une fonction positive ou nulle *et continue* est nulle, la fonction est identiquement nulle. Comme $P^2(x)/\sqrt{x} \geq 0$, l'intégrale sur $[1/2, 1]$ (par exemple) est inférieure ou égale à l'intégrale sur $[0, 1]$, donc à 0, et supérieure ou égale à 0, donc égale à 0. Il en résulte que $P(x)$ est identiquement nul sur $[1/2, 1]$, donc que le polynôme P a une infinité de racines, donc est identiquement nul. On aurait pu raisonner directement sur l'intervalle $[0, 1]$, mais le raisonnement ci-dessus évite d'utiliser (en fait redémontre) un théorème sur les intégrales généralisées.

2) Comme P_0 est de degré 0 et unitaire, on a $P_0(x) = 1$. On a $P_1(X) = X + aP_0(X)$, où a est déterminé par la condition $< P_1, P_0 >= 0$, d'où $a = - < P_0, X > / < P_0, P_0 >$. On a

$$< P_0, P_0 >= \int_{0,1} \frac{1}{\sqrt{x}}\, dx = 2 \quad \text{et} \quad < P_0, X >= \int_{0,1} \sqrt{x}\, dx = \frac{1}{3}\ ,$$

d'où $a = -1/3$, donc $P_1(X) = X - 1/3$.

Enfin, $P_2(X) = X^2 + bP_1(X) + cP_0(X)$, d'où

$$c = -\frac{< X^2, P_0 >}{< P_0, P_0 >} = -\frac{2/5}{2} = -\frac{1}{5}\ .$$

D'autre part

$$< P_1, P_1 >= \int_0^1 \frac{x^2 - (2/3)x + 1/9}{x^{1/2}}\, dx = \frac{2}{5} - \frac{4}{9} + \frac{2}{9} = \frac{8}{45}\ ,$$

et

$$< X^2, P_1 >= \int_0^1 \frac{x^3 - (1/3)x^2}{x^{1/2}}\, dx = \frac{2}{7} - \frac{2}{15} = \frac{16}{105}\ .$$

Il en résulte que

$$b = -\frac{< X^2, P_1 >}{< P_1, P_1 >} = -\frac{16/105}{8/45} = -6/7 \; .$$

On a donc

$$P_2(X) = X^2 - \frac{6}{7}\left(X - \frac{1}{3}\right) - \frac{1}{5} = X^2 - \frac{6}{7}X + \frac{3}{35} \; .$$

3) a) D'après la formule du binôme, on a

$$X^{n-1/2}(X-1)^n = \sum_{0\leq k\leq n} a_k X^{n+k-1/2}$$

où les a_k sont essentiellement les coefficients du binôme, mais dont la seule propriètè dont nous ayons besoin pour l'instant est que $a_n = 1$. La dérivée n-ième de X^a pour tout nombre réel a non entier est égale à une constante non nulle fois X^{a-n}, donc la dérivée n-ième de $X^{n-1/2}(X-1)$ est de la forme $\sum_{0\leq k\leq n} b_k X^{k-1/2}$ pour d'autres constantes b_k avec $b_n \neq 0$. Il en résulte que $Q_n(X) = \sum_{0\leq k\leq n} b_k X^k$, ce qui est donc un polynôme de degré exactement égal à n.

b) Par intégration par parties, on a

$$\begin{aligned} < Q_n, A > &= \int_0^1 A(x)\frac{d^n}{dx^n}(x^{n-1/2}(x-1)^n)\,dx \\ &= A(x)\frac{d^{n-1}}{dx^{n-1}}(x^{n-1/2}(x-1)^n)\Big|_0^1 - \int_0^1 \frac{d}{dx}A(x)\frac{d^{n-1}}{dx^{n-1}}(x^{n-1/2}(x-1)^n)\,dx \; . \end{aligned}$$

Appliquons la formule de Leibnitz au calcul de la dérivée k-ième de $x^{n-1/2}(x-1)^n$ pour $k < n$. La formule est une combinaison linéaire de produit de dérivées de $x^{n-1/2}$ d'ordre inférieur ou égal à k avec des dérivées de $(x-1)^n$ d'ordre inférieur ou égal à k. Quand $j < n$, la dérivée j-ième de $x^{n-1/2}$ est nulle en $x = 0$, et la dérivée j-ième de $(x-1)^n$ est nulle en $x = 1$. Il en résulte que la dérivée k-ième de $x^{n-1/2}(x-1)^n$ est nulle en $x = 0$ et en $x = 1$, quand $k < n$. Ceci signifie que le terme tout intégré est nul, donc que

$$< Q_n, A >= -\int_0^1 \frac{d}{dx}A(x)\frac{d^{n-1}}{dx^{n-1}}(x^{n-1/2}(x-1)^n)\,dx \; .$$

Par récurrence, on en déduit que pour tout $k \leq n$ on a

$$< Q_n, A >= (-1)^k \int_0^1 \frac{d^k}{dx^k}A(x)\frac{d^{n-k}}{dx^{n-k}}(x^{n-1/2}(x-1)^n)\,dx \; .$$

En particulier, si A est un polynôme de degré inférieur ou égal à $n-1$, la dérivée n-ième de A est nulle donc $< Q_n, A >= 0$.

c) Supposons par récurrence $P_0, \ldots, P_{n-1}$ construits. Le polynôme P_n est l'unique polynôme unitaire de degré n et orthogonal aux P_j pour $j < n$. D'après ce que nous venons de voir, Q_n est orthogonal aux P_j pour $j < n$, et c'est un polynôme de degré exactement égal à n. Si on pose $c_n = 1/b_n$, où b_n est le coefficient de degré n de Q_n, le polynôme $c_nQ_n(X)$ répond à toutes les conditions, et donc par unicité on a $P_n(X) = c_nQ_n(X)$.

D'après le calcul fait ci-dessus, on voit que

$$b_n = (2n-1/2)(2n-3/2)\cdots(n+1/2) = \frac{(4n-1)(4n-3)\cdots(2n+1)}{2^n} .$$

Or, pour tout entier m, on a

$$f(m) = (2m-1)(2m-3)\cdots 1 = \frac{(2m)!}{2m(2m-2)\cdot 2} = \frac{(2m)!}{2^m m!} .$$

Il en résulte que

$$b_n = \frac{f(2n)}{2^n f(n)} = \frac{(4n)!n!}{2^{2n}((2n)!)^2} .$$

On a donc finalement

$$c_n = \frac{1}{b_n} = \frac{2^{2n}((2n)!)^2}{(4n)!n!} .$$

4) a) Comme P_n et P_{n+1} sont unitaires, en regardant les termes de degré $n+1$ on constate que $u_n = 1$.

b) On a

$$X^{n-1/2}(X-1)^n = \sum_{0\le k\le n} \binom{n}{k}(-1)^{n-k}X^{n+k-1/2} .$$

D'autre part, pour $m \ge n$ on a

$$\begin{aligned}
\frac{d^n}{dX^n}X^{m-1/2} &= (m-1/2)(m-3/2)\cdots(m-n+1/2)X^{m-n-1/2} \\
&= \frac{(2m-1)(2m-3)\cdots(2m-2n+1)}{2^n}X^{m-n-1/2} \\
&= \frac{f(m)}{f(m-n)2^n}X^{m-n-1/2} = \frac{(2m)!(m-n)!}{m!(2m-2n)!2^{2n}}X^{m-n-1/2} ,
\end{aligned}$$

en utilisant la notation et la formule pour la fonction $f(m)$ introduite à la question précédente (on retrouve bien la formule pour b_n quand $m = 2n$). On a donc

$$\begin{aligned}
Q_n(X) &= \sum_{0\le k\le n}(-1)^{n-k}\frac{n!}{k!(n-k)!}\,\frac{(2n+2k)!k!}{(n+k)!(2k)!2^{2n}}X^k \\
&= \sum_{0\le k\le n}(-1)^{n-k}\frac{(2n+2k)!n!}{(n+k)!(n-k)!(2k)!2^{2n}}X^k ,
\end{aligned}$$

d'où

$$P_n(X) = c_nQ_n(X) = \sum_{0\le k\le n}(-1)^{n-k}\frac{(2n+2k)!((2n)!)^2}{(4n)!(n+k)!(n-k)!(2k)!}X^k .$$

A titre de vérification, on voit que le coefficient de X^n est bien égal à 1.

c) Le coefficient de X^n dans P_{n+1} vaut par définition a_{n+1}. Il n'y a pas de coefficient de X^n dans P_{n-1}, et le coefficient de X^n dans $(X+v_n)P_n(X)$ est égal à a_n+v_n. On a donc

$$v_n = a_{n+1} - a_n \ .$$

De même, le coefficient de X^{n-1} dans P_{n+1} vaut par définition b_{n+1}, et le coefficient de X^{n-1} dans $(X+v_n)P_n(X)+w_nP_{n-1}(X)$ est égal à $b_n+v_na_n+w_n$, d'où

$$w_n = b_{n+1} - b_n - a_n v_n = b_{n+1} - b_n - a_n(a_{n+1}-a_n) \ .$$

d) Le coefficient a_n s'obtient en prenant $k=n-1$ et b_n en prenant $k=n-2$ dans la formule explicite pour P_n trouvée ci-dessus. On obtient donc

$$a_n = -\frac{(4n-2)!((2n)!)^2}{(4n)!(2n-1)!(2n-2)!} = -\frac{(2n)(2n(2n-1))}{4n(4n-1)} = -\frac{n(2n-1)}{4n-1}$$

d'où

$$v_n = a_{n+1} - a_n = \frac{8n^2+4n-1}{(4n-1)(4n+3)} \ .$$

De même

$$\begin{aligned} b_n &= \frac{(4n-4)!((2n)!)^2}{2(4n)!(2n-2)!(2n-4)!} = \frac{(2n)(2n-1)((2n)(2n-1)(2n-2)(2n-3))}{2(4n)(4n-1)(4n-2)(4n-3)} \\ &= \frac{n(n-1)(2n-1)(2n-3)}{2(4n-1)(4n-3)} \end{aligned}$$

d'où

$$w_n = b_{n+1} - b_n - a_n v_n = -4\frac{n^2(2n-1)^2}{(4n+1)(4n-1)^2(4n-3)} \ .$$

Exercice II

1) Soit $A=UDV^t$ une décomposition de A en valeurs singulières, avec U et V orthogonales et D diagonale. Nous savons que pour toute matrice orthogonale U, les normes de UM et de MU sont égales à la norme de M (car une matrice orthogonale fournit une bijection de la sphère unité sur elle-même). Il en résulte que la norme de A est égale à la norme de la matrice diagonale D. Mais il est évident que la norme d'une matrice diagonale est égal à la plus grande valeur absolue (ou module dans le cas complexe) de ses coefficients diagonaux. Les coefficients diagonaux non nuls de D étant par définition les valeurs singulières de A, on en déduit le résultat.

2) a) On calcule que $A^tA = 75J$ où

$$J = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} .$$

Comme U est orthogonale, on en déduit que $75J = VD^2V^t$. Les valeurs propres de $75J$ sont trivialement 0 (double) et $75 \cdot 3 = 225$ (simple), d'où

$$D = \begin{pmatrix} 15 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} .$$

Pour obtenir une matrice V, il faut chercher une *base orthonormée* de vecteurs propres de A^tA (n'importe quelle base ne conviendrait pas). Un vecteur propre pour la valeur propre 225 est le vecteur $(1,1,1)^t$, d'où on doit prendre $v_1 = (1/\sqrt{3})(1,1,1)^t$. Une base de vecteurs propres pour la valeur propre nulle est par exemple formée des vecteurs $(1,-1,0)^t$ et $(1,0,-1)^t$, qui sont automatiquement orthogonaux à v_1 (savez-vous pourquoi ?). Appliquant le procédé de Gram–Schmidt à cette base pour trouver une base orthonormée (et pas seulement orthogonale), on trouve $v_2 = (1/\sqrt{2})(1,-1,0)^t$ et $v_3 = (1/\sqrt{6})(1,1,-2)$, d'où

$$V = \frac{1}{\sqrt{6}} \begin{pmatrix} \sqrt{2} & \sqrt{3} & 1 \\ \sqrt{2} & -\sqrt{3} & 1 \\ \sqrt{2} & 0 & -2 \end{pmatrix} .$$

D'autre part, on calcule que

$$AA^t = \begin{pmatrix} 3 & 15 & 21 \\ 15 & 75 & 105 \\ 21 & 105 & 147 \end{pmatrix} .$$

Nous savons déjà que les valeurs propres de cette matrice sont 0 (double) et 225 (simple). Un vecteur propre correspondant à 225 est $(1,5,7)^t$, d'où $u_1 = (1/(5\sqrt{3}))(1,5,7)^t$ est le premier vecteur propre normalisé.

Une base de vecteurs propres pour la valeur propre nulle est par exemple formée des vecteurs $(7,0,-1)^t$ et $(5,-1,0)^t$, qui sont automatiquement orthogonaux à u_1. Appliquant Gram–Schmidt, on trouve $u_2 = (1/(5\sqrt{2}))(7,0,-1)^t$ et $u_3 = (1/(5\sqrt{6}))(1,-10,7)^t$, d'où

$$U = \frac{1}{5\sqrt{6}} \begin{pmatrix} \sqrt{2} & 7\sqrt{3} & 1 \\ 5\sqrt{2} & 0 & -10 \\ 7\sqrt{2} & -\sqrt{3} & 7 \end{pmatrix} .$$

Noter que les matrices U et V trouvées ci-dessus donnent *une* décomposition SVD, mais ne sont pas unique, donc dans un autre corrigé on aurait pu prendre d'autres matrices. Seule les valeurs singulières (les éléments diagonaux de D) sont uniques.

b) La norme de A est égale à la plus grande valeur singulière, donc à 15.

3) Par définition, $A^\dagger = VD^\dagger U^t$, où

$$D^\dagger = \begin{pmatrix} 1/15 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} .$$

Tous calculs faits, on trouve que

$$A^\dagger = \frac{1}{225} \begin{pmatrix} 1 & 5 & 7 \\ 1 & 5 & 7 \\ 1 & 5 & 7 \end{pmatrix} .$$

On voit que ce n'est autre que la transposée de A divisée par 225. Ceci aurait pu se voir sans calculs. En effet, on sait que $A^\dagger$ est caractérisée par le fait que $AA^\dagger$ et $A^\dagger A$ sont des matrices symétriques, ce qui est clair quand $A^\dagger$ est proportionelle à A^t, et telles que $AA^\dagger A = A$ et $A^\dagger AA^\dagger = A^\dagger$, ce qui se vérifie immédiatement.

Exercice III

1) a) On a clairement $M(a,b) - M(a',b') = M(a-a', b-b')$ donc A est un sous-groupe. D'autre part $M(1,0)$ est l'identité I. Enfin, si on pose $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, on a $J^2 = -I$, et $M(a,b) = aI + bJ$ donc $M(a,b)M(a',b') = M(aa' - bb', ab' + ba')$ donc A est stable par multiplication, et est donc bien un sous-anneau.

b) Comme $M(a',b')M(a,b) = M(a'a - b'b, a'b + b'a) = M(a,b)M(a',b')$, il est clair que A est commutatif (on peut aussi dire que I et J commutent entre eux, ce qui est suffisant).

2) a) On remarque que $M(\lambda a, \lambda b) = \lambda M(a,b)$. Il en résulte que

$$M^2 = M(a^2 - b^2, 2ab) = 2aM(a,b) - (a^2+b^2)M(1,0) = 2aM - (a^2+b^2)I .$$

On peut aussi obtenir ce résultat sans calcul : d'après le théorème de Cayley–Hamilton, M est racine de son polynôme caractéristique. Comme la trace de M vaut $2a$ et son déterminant vaut $a^2 + b^2$, on obtient le même résultat.

b) Multipliant par M^{n-1}, on obtient la relation

$$M^{n+1} = 2aM^n - (a^2+b^2)M^{n-1} .$$

c) Comme $M^n = u_n I + v_n J$, de la relation ci-dessus on obtient

$$u_{n+1}I + v_{n+1}J = 2a(u_n I + v_n J) - (a^2+b^2)(u_{n-1}I + v_{n-1}J) ,$$

et comme I et J sont des matrices linéairement indépendantes, on en déduit que u_n et v_n satisfont à la même rcurrence que M^n, à savoir $x_{n+1} = 2ax_n - (a^2+b^2)x_{n-1}$. On a $M^0 = I$ donc $u_0 = 1$, $v_0 = 0$, et $M^1 = M = aI + bJ$ donc $u_1 = a$, $v_1 = b$.

3) a) Déjà fait : nous avons vu que $J^2 = -I$.

b) D'après la formule du binôme de Newton, que nous pouvons appliquer dans l'anneau A puisqu'il est *commutatif*, on a

$$M(a,b)^p = (aI+bJ)^p = \sum_{0\le k\le p} \binom{p}{k} a^k b^{p-k} I^k J^{p-k} = \sum_{0\le k\le p} \binom{p}{k} a^k b^{p-k} J^{p-k} .$$

Or quand p est un nombre premier, les coefficients binomiaux $\binom{p}{k}$ sont tous divisibles par p sauf les deux extrêmes pour $k=0$ et $k=p$, qui sont égaux à 1. Comme nous sommes en caractéristique p, il en résulte que $\binom{p}{k} \cdot 1_{\mathbb{F}_p} = 0$ pour $1 \le k \le p-1$, d'où

$$M(a,b)^p = a^p I^p + b^p J^p = a^p I + b^p J^p .$$

Nous venons de redémontrer que l'application $x \to x^p$ est une application linéaire dans un anneau commutatif de caractéristique p, résultat qu'on aurait pu utiliser directement sans démonstration.

Continuant le calcul, comme $J^2 = -I$, on en déduit que $J^4 = I$ donc, comme $p \equiv 3 \pmod 4$ que $J^{p-3} = I$, donc que $J^{p-1} = J^2 = -I$, d'où enfin $J^p = -J$. D'autre part, nous savons que tout élément du corps $\mathbb{F}_p$ vérifie $a^p = a$ (par exemple, on peut dire que si $a \neq 0$, on a $a^{p-1} = 1$ d'après Fermat, mais c'est une propriété fondamentale de $\mathbb{F}_p$). Attention, ceci est spécifique à $\mathbb{F}_p$, et n'est *pas* vrai dans un corps quelconque de caractéristique p, contrairement à la linéarité de $x \to x^p$. On en déduit donc finalement que $M(a,b)^p = aI - bJ$.

c) On a donc

$$M(a,b)^{p+1} = M \cdot M^p = (aI+bJ)(aI-bJ) = a^2 I - b^2 J^2 = (a^2+b^2) I .$$

Il en résulte que $u_{p+1} = a^2 + b^2$ et que $v_{p+1} = 0$.

4) a) Appelons x_n la classe de z_n dans $\mathbb{Z}/p\mathbb{Z}$. On a donc la récurrence $x_{n+1} = 2ax_n - (a^2+b^2)x_{n-1}$ avec les conditions initiales $x_0 = 0$ et $x_1 = b$. Or une suite récurrente d'ordre 2 comme celle-ci est déterminée de manière unique par les conditions initiales et la récurrence. Comme celles-ci sont les mêmes que celles de la suite v_n vues ci-dessus, on en déduit que $x_n = v_n$, donc v_n est bien la classe de z_n dans $\mathbb{Z}/p\mathbb{Z}$.

b) D'après la question 3c) on sait que $v_{p+1} = 0$, et comme v_n est la classe de z_n, ceci signifie que $z_{p+1} \equiv 0 \pmod p$.

5) Le nombre $p = 23$ est bien premier et congru à 3 modulo 4. Pour appliquer la question précédente à la récurrence donnée, il nous faut choisir α et β dans $\mathbb{Z}$ tels que la classe de 2α modulo 23 soit égal à 1, ce qui donne $\alpha = 12$, et la classe de $\alpha^2 + \beta^2$ modulo 23 soit égal à -1, ce qui est bien vérifié pour $\beta = 4$ puisque $12^2 + 4^2 = 160 \equiv -1 \pmod{23}$. La suite z_n est la suite vérifiant la récurrence donnée (modulo 23) avec les conditions initiales $z_0 = 0$ et $z_1 = 4$, donc par unicité $z_n \equiv 4F_n \pmod{23}$ puisque ceci est vrai pour $n = 0$ et $n = 1$. On déduit de la question précédente que $4F_{24} \equiv 0 \pmod{23}$, d'où $F_{24} \equiv 0 \pmod{23}$ puisque 4 est inversible modulo 23.