Université Bordeaux 1
Mathématiques

MAT812 – Calcul Formel
Année 2009–2010

Examen, 05 mai 2010, 08:00 – 11:00.

Durée 3 heures. Documents interdits, calculettes autorisées.

Le barème (sur 20) est indicatif.

Exercice 1 – (5 points). Soit I l'idéal de $\mathbb{C}[x,y,z]$ engendré par les polynômes $x+y+z$, y^2+yz+z^2 et z^3.

1) Montrer par l'absurde que $1 \notin I$. On pourra écrire une relation de dépendance et évaluer en $(0,0,0)$.

2) On choisit l'ordre lexicographique sur les monômes de $\mathbb{C}[x,y,z]$, avec $x > y > z$. Calculer un reste de la division de x^2+xy^2 par les 3 polynômes ci-dessus. On rappellera la condition que doit vérifier le reste.

3) Étant donné $f \in \mathbb{C}[x,y,z]$, on cherche à décider si $f \in I$ par division euclidienne par les polynômes de la base. Que peut-on dire dans les trois situations suivantes :

a) le reste obtenu est 0.

b) le reste obtenu est 1.

c) le reste obtenu est x. [*Attention au piège !*]

Exercice 2 – (2 points). On désire trouver tous les polynômes $A, B, C \in \mathbb{F}_2[x]$ tels que

$$(*) \qquad (x+1)A + x^2B + C = 1$$

Un algorithme de type Euclide[1] fournit une matrice $U \in \mathrm{SL}_3(\mathbb{F}_2[x])$, c'est-à-dire 3×3 à coefficients dans $\mathbb{F}_2[x]$ et de déterminant 1, telle que

$$\begin{pmatrix}(x+1) & x^2 & 1\end{pmatrix} U = \begin{pmatrix}1 & 0 & 0\end{pmatrix}.$$

On pose

$$\begin{pmatrix}a\\ b\\ c\end{pmatrix} := U^{-1}\begin{pmatrix}A\\ B\\ C\end{pmatrix}.$$

Décrire l'ensemble des $a, b, c \in \mathbb{F}_2[x]$ et en déduire l'ensemble des (A, B, C) solutions de l'équation $(*)$.

[1] convenablement généralisé. *On ne demande pas de décrire un tel algorithme, ni de calculer U.*

Problème (13 points)

Soit $N > 1$ un entier dont on désire montrer qu'il est *premier*.

1) Soit $p \mid N-1$ un nombre premier et $e = v_p(N-1)$ la plus grande puissance de p divisant $N-1$. On suppose qu'il existe $a = a(p) \in \mathbb{Z}$ vérifiant

- $a^{N-1} \equiv 1 \pmod{N}$,
- $\mathrm{pgcd}\left(a^{(N-1)/p} - 1, N\right) = 1$.

Dans cette question, on veut montrer que tout diviseur d de N vérifie $d \equiv 1 \pmod{p^e}$.

a) Montrer qu'il suffit de démontrer l'assertion pour tout diviseur d *premier*.

b) Soit d un diviseur premier de N, on note o l'ordre de a dans $(\mathbb{Z}/d\mathbb{Z})^*$. Montrer que o divise $N-1$, mais qu'il ne divise pas $\frac{N-1}{p}$.

c) En déduire que $p^e \mid o$ et conclure.

2) On suppose que $N - 1 = FU$, où $F \geqslant \sqrt{N}$ est un facteur dont tous les diviseurs premiers sont connus, tel que $(F, U) = 1$. On suppose que pour chaque diviseur premier p de F, on connaît $a(p)$ vérifiant les propriétés du 1). Soit $d > 1$ un diviseur de N.

a) Montrer que $d \equiv 1 \pmod{F}$. [*Utiliser le 1) et penser au Lemme Chinois.*]

b) En déduire que $d > \sqrt{N}$, puis que N est premier.

c) On suppose N premier, et on fixe $p \mid N-1$. Tirant a uniformément au hasard dans $[1, N-1]$, montrer que la probabilité qu'il satisfasse les propriétés demandées pour $a(p)$ ci-dessus est

$$1 - \frac{1}{p} \geqslant \frac{1}{2}.$$

[*Montrer que le nombre de a tel que $a^{(N-1)/p} \equiv 1 \pmod{N}$ est $(N-1)/p$.*]

d) Écrire un algorithme certifiant la primalité en utilisant les principes ci-dessus. Il prend en entrée un nombre premier N, une factorisation $N - 1 = FU$ vérifiant les propriétés ci-dessus, où la liste des diviseurs premiers de F est donnée. Il doit renvoyer en sortie la liste des $a(p)$ pour $p \mid F$.

e) Borner la complexité en moyenne de votre algorithme en fonction de N.

3) En gardant les mêmes notations que ci-dessus, on suppose maintenant que $N - 1 = FU$, avec

$$N^{1/3} \leqslant F < N^{1/2},$$

et que pour tout diviseur premier p de F est donné un $a(p)$ comme ci-dessus.

a) Prouver que la décomposition en base F de N est de la forme $c_2F^2 + c_1F + 1$, avec $c_i \in [0, F-1]$.

b) On suppose dans cette question et la suivante que N n'est pas premier. Montrer que N a exactement deux diviseurs premiers (éventuellement égaux), de la forme

$$p = aF + 1, \quad q = bF + 1,$$

pour des entiers $a, b > 0$. On peut supposer, et nous le ferons dans la suite, que $a \leqslant b$.

c) Toujours en supposant N non premier, prouver que $ab \leqslant F - 1$; en déduire que $a + b \leqslant F - 1$ *ou* ($a = 1$ et $b = F - 1$). Montrer en développant $p \times q$ que ce deuxième cas est en fait impossible, et donc que $c_1 = a + b$ et $c_2 = ab$.

d) Montrer que N est premier *si et seulement si* $c_1^2 - 4c_2$ n'est pas un carré dans $\mathbb{Z}$.