Université Bordeaux 1 — **MAT823 – Calcul Formel**
Mathématiques — Année 2012–2013

Examen, 04 mai 2007, 8h30 – 11h30

Durée 3 heures. Documents interdits, calculettes autorisées.

Les trois exercices d'application et le problème sont indépendants. *On demande que les questions 1.a) et 1.b) du Problème soient abordées.*

Exercice 1 – Soit $N = 187$ et $\mathcal{B} = \{2, 3, 5\}$. On remarque que dans $\mathbb{Z}/N\mathbb{Z}$, on a

$$\begin{aligned} 37^2 &= 2^2 \times 3 \times 5, \\ 149^2 &= 3^3 \times 5, \\ 163^2 &= 3 \times 5. \end{aligned}$$

En *déduire* une identité $x^2 = y^2$ exhibant un facteur non trivial de N.

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

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

1) Trouver une matrice $U \in \mathrm{GL}_3(\mathbb{F}_2[x])$, c'est-à-dire 3×3 et inversible, telle que

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

2) 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 $(*)$.

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

1) 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.

2) 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. [*Montrer par l'absurde que* $1 \notin I$.]

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

Problème (Preuve de primalité)

Soit $N > 1$ un entier. Soit $p \mid N-1$ un nombre premier et $e := v_p(N-1)$, c'est-à-dire que p^e divise exactement $N-1$. On suppose qu'il existe $a \in \mathbb{Z}$ vérifiant

$$(S_p) \qquad \begin{cases} a^{N-1} \equiv 1 \pmod{N}, \\ \operatorname{pgcd}\left(a^{(N-1)/p} - 1, N\right) = 1. \end{cases}$$

Sous ces conditions, tout diviseur d de N vérifie $d \equiv 1 \pmod{p^e}$. [*On ne demande pas de reproduire cette démonstration.*]

1) On fixe N et p et on se donne un entier $0 < a < N$.

a) Proposer un code Maple testant si a vérifie bien les conditions (S_p).

b) Borner le nombre d'opérations élémentaires utilisées par votre algorithme, en fonction de $n := \log N$. [*On pourra supposer qu'addition et multiplication dans $\mathbb{Z}/N\mathbb{Z}$ utilisent $\widetilde{O}(n)$ opérations élémentaires, ainsi que le calcul de* $\operatorname{pgcd}(u,v)$ *quand* $|u|, |v| < N$.]

2) Dans toute cette question, on suppose que N est premier, et on fixe un nombre premier p divisant $N-1$.

a) Comment se simplifient les deux propriétés (S_p) ?

b) En déduire la probabilité qu'un entier a tiré uniformément au hasard dans $[1, N]$ vérifie (S_p). S'attend-on à trouver rapidement de tels a ?

On suppose dans toute la suite que $N - 1 = FU$, où tous les facteurs premiers de F sont connus, et que pour chaque $p \mid F$, on connaît $a = a(p)$ vérifiant les propriétés (S_p).

3) On suppose dans cette question que $F \geqslant N^{1/2}$. Soit $d > 1$ un diviseur de N.

a) Montrer que $d \equiv 1 \pmod{F}$.

b) En déduire que $d > N^{1/2}$, puis que N est premier.

4) On suppose maintenant que $N^{1/3} \leqslant F < N^{1/2}$.

a) Démontrer que la décomposition en base F de N est de la forme $c_2F^2 + c_1F + 1$.

b) On suppose que N n'est pas premier. Montrer qu'il a exactement deux diviseurs premiers de la forme $p = aF + 1$, $q = bF + 1$, pour des entiers $0 < a \leqslant b$. Montrer que $ab \leqslant F - 1$ et en déduire que $a + b \leqslant F - 1$ [*montrer que le cas $a = 1$, $b = F - 1$ est impossible*], puis que $c_1 = a + b$, $c_2 = ab$. Conclure que $c_1^2 - 4c_2$ est un carré dans $\mathbb{Z}$.

c) Avec les notations du a), montrer que N est premier si et seulement si $c_1^2 - 4c_2$ n'est pas un carré dans $\mathbb{Z}$.

5) Écrire une procédure Maple complète qui prend en entrée un entier N et une liste L_F de nombres premiers divisant $N-1$, et prouve la primalité de N grâce aux méthodes du 3) et du 4), si l'entier F correspondant est suffisamment grand. Il est interdit d'utiliser les fonctions de type `factor`.