université de BORDEAUX	**ANNEE UNIVERSITAIRE 2014/2015** **Examen seconde session** **Master 1** **Code UE : MSIN820, MSMA820** **Epreuve : Algèbre et calcul formel** **Date : 23/06/2015** **Heure : 14h00** **Durée : 3h** Documents autorisés : Feuilles d'exercices (énoncés). Epreuve de M. Jehanne	**Collège Sciences et technologies**

Exercice 1

Dans cet exercice, il est conseillé d'utiliser sage pour certains calculs. Pour chacun de ces calculs, il est demandé d'écrire sur votre copie les commandes utilisées et les résultats obtenus.

Dans $\mathbb{Q}[x,y]$, on considère les polynômes suivants.

$$\begin{cases} f_1 = x^3 + y^3 - 3xy - 1 \\ f_2 = x^2 + y^2 - 4 \end{cases}$$

1. En utilisant une base de Gröbner (calculée à l'aide de sage), déterminer l'ensemble des $(x,y) \in \mathbb{R}^2$ tels que

$$f_1(x,y) = f_2(x,y) = 0.$$

Indiquez sur votre copie l'ordre sur les monômes choisi, la base de Gröbner obtenue et le raisonnement utilisé.

2. Donner une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[x,y]/I$.

3. Soit I l'idéal de $\mathbb{Q}[x,y]$ engendré par f_1 et f_2. Le polynôme $f = x^6 + y^6 - 28$ appartient-il à I ?

4. Écrire sur votre fichier sage un programme qui étant donnés une liste l de polynômes de $\mathbb{Q}[x,y]$ et un polynôme g de $\mathbb{Q}[x,y]$ indique si g appartient ou non à l'idéal de $\mathbb{Q}[x,y]$ engendré par les éléments de l.

Exercice 2

On rappelle qu'un entier n est appelé nombre de Carmichael s'il est composé et si pour tout entier a premier à n,

$$a^{n-1} \equiv 1 \mod n.$$

Commentaire. *Dans les questions 1 et 2 de cet exercice, on démontre le critère de Korselt, qui affirme qu'un nombre entier composé n est de Carmichael si et seulement s'il est sans facteur carré et si pour tout diviseur premier p de n, l'entier $p-1$ divise $n-1$.*

1. Soit p un nombre premier et m un entier naturel non nul. Soit $n = p^2 m$.

a) Montrer que $1 + pm$ est premier à n.

b) Montrer que

$$(1+pm)^{n-1} \not\equiv 1 \mod n.$$

c) En déduire que tout nombre de Carmichael est sans facteurs carrés.

2. On rappelle que si p est premier, $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique. Soit n un entier composé sans facteur carré.

a) On suppose que pour tout nombre premier p divisant n, l'entier $p-1$ divise $n-1$. Soit a un entier premier à n. Montrer que

$$a^{n-1} \equiv 1 \mod n.$$

En déduire que n est de Carmichael.

b) On suppose que n est de Carmichael. Soit p un diviseur premier de n. Soit g un entier dont la classe modulo p engendre $(\mathbb{Z}/p\mathbb{Z})^*$. Montrer qu'il existe un entier a premier à n tel que $a \equiv g \mod p$. Quel est l'ordre de $a \mod p$? Montrer que $p-1$ divise $n-1$.

3. Montrer que tout nombre de Carmichael est impair.

4. Montrer que tout nombre de Carmichael possède au moins trois diviseurs premiers.

5. Soit n un nombre de Carmichael. On pose $n-1 = 2^e q$, où q est impair. Soit a un entier premier à n. On suppose que a est un témoin de Rabin-Miller pour n, c'est-à-dire que

$$a^q \not\equiv 1 \mod n \quad \text{et} \quad a^{2^i q} \not\equiv -1 \ \forall i \in [[0, e-1]].$$

a) Montrer que $E = \{i \in \mathbb{N} \ : \ a^{2^i q} \equiv 1 \mod n\}$ est non vide.

b) Soit $m = \min E$. Montrer que $m \geq 1$ et que $\mathrm{pgcd}(a^{2^{m-1}q} - 1, n)$ est un facteur non trivial de n.

Exercice 3

On rappelle l'algorithme de Cantor-Zassenhaus en caractéristique impaire.

Algorithme de Cantor-Zassenhaus en caractéristique impaire.
Entrées. $q = p^k$, où p est un nombre premier impair, $Q \in \mathbb{F}_q[x]$ de degré n, produit de polynômes irréductibles deux à deux distincts de degré d.
Sortie. Un diviseur non trivial de Q, ou bien "Echec".

Tirer au hasard $A \in \mathbb{F}_q[x]$ de degré strictement inférieur à n.
Calculer $D = \mathrm{pgcd}(A, Q)$. Si $D \neq 1$, sortir D.
Calculer $B = A^{(q^d-1)/2} - 1 \mod Q$
Calculer $D = \mathrm{pgcd}(B, Q)$
Si $D \neq 1$ et $\deg D \neq \deg Q$, sortir D. Sinon, sortir "Echec".

1. Soit $m \geq 1$, et soit

$$T_m = x^{2^{m-1}} + x^{2^{m-2}} + \cdots + x^4 + x^2 + x \in \mathbb{F}_2[x].$$

a) Montrer que $T_m(T_m + 1) = x^{2^m} + x$.

b) En déduire que si $\alpha \in \mathbb{F}_{2^m}$, alors $T_m(\alpha) \in \mathbb{F}_2$.

c) Montrer que l'application $\alpha \mapsto T_m(\alpha)$ de $\mathbb{F}_{2^m}$ dans $\mathbb{F}_2$ est une application linéaire de $\mathbb{F}_2$-espaces vectoriels. En déduire que

$$\mathrm{Card}\{\alpha \in \mathbb{F}_{2^m} \ : \ T_m(\alpha) = 0\} = \mathrm{Card}\{\alpha \in \mathbb{F}_{2^m} \ : \ T_m(\alpha) = 1\} = 2^{m-1}.$$

2. Soient maintenant $q = 2^k$ et $Q \in \mathbb{F}_q[x]$ de degré n. On suppose que Q est produit de r polynômes irréductibles sur $\mathbb{F}_q$ qu'on note $P_1, \ldots, P_r$, deux à deux distincts et tous de même degré d. On note $R = \mathbb{F}_q[x]/(Q)$, $R_i = \mathbb{F}_q[x]/(P_i)$ et ϕ_i l'application canonique de R dans R_i définie par $\phi_i(P \mod Q) = P \mod P_i$.

a) Soit $A \in R$. Montrer que $\phi_i(T_{kd}(A)) \in \mathbb{F}_2$ pour tout i et que si A est choisi au hasard dans R avec probabilité uniforme, $T_{kd}(A)$ appartient à $\mathbb{F}_2$ avec probabilité 2^{1-r}.

b) En déduire un algorithme pour factoriser Q qui s'inspire de l'algorithme de Cantor-Zassenhaus ci-dessus, et dont la probabilité d'échec est inférieure à $1/2$.

c) Écrire cet algorithme sur votre fichier sage, dans le cas particulier où $q = 2$. On prendra soin de minimiser le temps de calcul. Pour tester votre fonction, vous pourrez d'abord utiliser des exemples simples, comme $Q = x^2 + x$ et $d = 1$, puis des exemples plus difficiles, comme $Q = (x^{64} + x + 1)/(x^4 + x + 1)$ et $d = 12$.