	ANNEE UNIVERSITAIRE 2015/2016 **Examen première session** **Master 1** **Code UE : MSIN820, MSMA820** **Epreuve : Algèbre et calcul formel** **Date : 10/05/2016** **Heure : 9h00** **Durée : 3h** Documents autorisés : Feuilles d'exercices (énoncés). Epreuve de M. Jehanne	**Collège Sciences et technologies**

À la fin de l'épreuve, votre fichier "`votre_nom.sage`" est à envoyer à l'adresse : `arnaud.jehanne@u-bordeaux.fr`

Exercice 1 [Bases de Gröbner]

Soit $\mathcal{C}$ la courbe de $\mathbb{R}^2$ définie par le paramétrage

$$\begin{cases} x(t) = \dfrac{t}{t^4+1} \\ y(t) = \dfrac{t^3}{t^4+1} \end{cases}$$

1. Soient $f = x(t^4+1)-t$ et $g = y(t^4+1)-t^3$ dans $\mathbb{Q}[t,x,y]$ et I l'idéal de $\mathbb{Q}[t,x,y]$ engendré par f et g. En utilisant la base de Gröbner réduite de I (que vous calculerez avec sage) correspondant à un ordre monomial bien choisi, déterminer un polynôme $P \in \mathbb{Q}[x,y]$ tel que $\mathbb{Q}[x,y] \cap I = P\mathbb{Q}[x,y]$. Vous indiquerez sur votre copie les commandes utilisées (donc en particulier l'ordre monomial choisi) et la base de Gröbner obtenue.
2. Montrer que $\mathcal{C} = \{(x,y) \in \mathbb{R}^2 \ : \ P(x,y) = 0\}$.

Exercice 2 [Factorisation en degrés distincts, Factorisation en degrés par intervalles]

Soit p un nombre premier. Soit f un polynôme non nul de $\mathbb{F}_p[x]$. Pour tout entier naturel non nul d et toute partie I de $\mathbb{N} \setminus \{0\}$, on définit les ensembles suivants.
$\mathrm{Irr}(f)$: l'ensemble des facteurs irréductibles unitaires de f dans $\mathbb{F}_p[x]$.
$\mathcal{D}_f(d)$: l'ensemble des éléments de $\mathrm{Irr}(f)$ dont le degré divise d.
$\mathcal{E}_f(d)$: l'ensemble des éléments de $\mathrm{Irr}(f)$ de degré d.
$\mathcal{D}_f(I)$: l'ensemble des éléments de $\mathrm{Irr}(f)$ dont le degré divise un élément de I.
$\mathcal{E}_f(I)$: l'ensemble des éléments de $\mathrm{Irr}(f)$ dont le degré appartient à I.
On rappelle que pour tout entier naturel non nul d,

$$\mathrm{pgcd}(x^{p^d} - x, f) = \prod_{Q \in \mathcal{D}_f(d)} Q$$

Soient P et Q deux polynômes de $\mathbb{F}_p[x]$ et soit n un entier naturel. Pour calculer rapidement P^n mod Q, utiliser la commande `power_mod(P,n,Q)`.
1. Dans tout l'exercice, on suppose que $\mathrm{pgcd}(f, f') = 1$. Montrer que f est sans facteurs carrés.
2. On définit les suites de polynômes (g_i) et (f_i) en posant $g_0 = 1$, $f_0 = f$, et pour tout $i \in \mathbb{N} \setminus \{0\}$,

$$g_i = \mathrm{pgcd}(x^{p^i} - x, f_{i-1}) \quad \text{et} \quad f_i = \frac{f_{i-1}}{g_i}.$$

Montrer que pour tout entier naturel i non nul,

$$g_i = \prod_{Q \in \mathcal{E}_f(i)} Q$$

3. a) Soit $s = \max\{\deg Q \ : \ Q \in \mathrm{Irr}(f)\}$. Écrire sur votre ficher `.sage` une fonction `DegDist` qui en entrée prend un nombre premier p et un polynôme $f \in \mathbb{F}_p[x]$ sans facteurs carrés, et qui en sortie rend la liste $[g_0, g_1, \ldots, g_s]$. Cette liste est appelée *factorisation en degrés distincts* de f. On s'efforcera de minimiser le temps de calcul. On pourra essayer cette fonction `DegDist` sur les polynômes $f_1 = x^{10} + x + 1$ et $f_2 = x^{601} + x^{600} + x - 1$ de $\mathbb{F}_3[x]$ (cela ne doit pas prendre plus de quelques secondes). On ne demande pas le résultat de ces calculs.

b) Écrire sur votre fichier `.sage` une fonction `DegDistDeg` qui avec les mêmes entrées rend la liste $[[i, \deg g_i] \ : g_i \neq 1]$.

c) Sachant que `DegDistDeg`, appliquée à f_1 (resp. f_2) donne $[[1,1],[3,3],[6,6]]$ (resp. $[[3,3],$ $[10,20]$,$[90,90]$, $[488,488]]$), décider si la fonction `DegDist` donne ou pas la factorisation complète de f_1 (resp. f_2).

4. Écrire sur votre fichier `.sage` une fonction `Suite` qui en entrée prend un entier naturel non nul n et en sortie rend la liste $[1, 2, 4, \ldots, 2^{t-1}, n]$ où t est l'entier tel que $2^{t-1} < n \leq 2^t$.

5. Soit I un intervalle fini de $\mathbb{N} \setminus \{0\}$. Montrer que

$$\mathrm{pgcd}\left(\prod_{d\in I}\left(x^{p^d} - x\right), f\right) = \prod_{Q\in\mathcal{D}_f(I)} Q$$

6. Soit $(a_i)_{i\in\mathbb{N}}$ une suite strictement croissante d'entiers. Pour tout $i \in \mathbb{N}$, on pose

$$I_i = [[a_i, a_{i+1} - 1]] \quad \text{et} \quad h_i = \prod_{Q\in\mathcal{E}_f(I_i)} Q$$

Montrer que si $a_k > \deg f$, alors $h_k = 1$ (on rappelle qu'un produit vide est égal à 1).

7. On suppose que $a_0 = 1$. On définit les suites $(H_i)_{i\geq -1}$ et $(F_i)_{i\geq -1}$ en posant $H_{-1} = 1$, $F_{-1} = f$ et pour tout $i \in \mathbb{N}$

$$H_i = \mathrm{pgcd}\left(\prod_{d\in I_i}\left(x^{p^d} - x\right), F_{i-1}\right) \quad \text{et} \quad F_i = \frac{F_{i-1}}{H_i}$$

Montrer que $H_i = h_i$ pour tout $i \in \mathbb{N}$.

8. Écrire sur votre fichier `.sage` une fonction `DegInter` qui en entrée prend un nombre premier p, un polynôme sans facteurs carrés f et une liste $[a_0, \ldots, a_t]$ où $1 = a_0 < a_1 < \cdots < a_t$ et en sortie rend la liste $[h_0, \ldots, h_{t-1}]$ correspondante. On s'efforcera de minimiser le temps de calcul. On pourra essayer cette fonction sur la suite $(2^i)_{i\in\mathbb{N}}$ (en utilisant votre fonction `Suite`) et les polynômes $f_3 = x^{12} + x^6 + x - 1$, puis $f_4 = x^{1000} + x - 1$ de $\mathbb{F}_3[x]$ (cela ne doit prendre que quelques secondes).

9. a) Pour $i \in \mathbb{N}$, on pose $a_i = 2^i$, et on considère les h_i correspondants. Montrer que h_i est irréductible si et seulement si $\deg h_i \in I_i$ (où $I_i = [[2^i, 2^{i+1} - 1]]$).

b) Quelle est la liste $[[i, \deg h_i] \ : \ h_i \neq 1]$ correspondant au polynôme f_3 (resp. f_4) ? Déduire de cette liste si `DegInter` donne la factorisation complète de f_3 (resp. f_4) ou non.

Exercice 3 [À propos du théorème de Rabin-Miller]

On rappelle l'énoncé de ce théorème.

Théorème (Rabin-Miller). *Soit n un nombre premier impair. Soit $(e, q) \in \mathbb{N}^2$ le couple d'entiers tel que $n - 1 = 2^e q$ et $q \equiv 1 \mod 2$. Soit a un entier premier à n, alors*

(i) soit $a^q \equiv 1 \mod n$,

(ii) soit il existe $i \in [[0, e-1]]$ tel que $a^{2^i q} \equiv -1 \mod n$.

On rappelle aussi qu'un entier n est appelé *nombre de Carmichael* s'il est composé et si pour tout entier a premier à n, $a^{n-1} \equiv 1 \mod n$. Nous avons vu qu'un tel nombre est sans facteur carré.

Soit n un entier impair composé. Pour tout entier a, on note $[a]_n$ la classe de a modulo n. Si a est un entier qui ne vérifie aucune des condition (i) ou (ii) du théorème, on dit que a et $[a]_n$ sont des *témoins de non primalité* pour n. S'il vérifie l'une de ces conditions, on dit que a et $[a]_n$ sont des *faux témoins de primalité* pour n. Nous allons démontrer le résultat suivant (nous avons vu un résultat plus fort en cours mais avec une preuve différente, et plus difficile).

Théorème. *Soit $M(n)$ l'ensemble des faux témoins de primalité pour n de $\mathbb{Z}/n\mathbb{Z}$. Alors*

$$\mathrm{Card} M(n) \leq \frac{\varphi(n)}{2}$$

où $\varphi = \mathrm{Card}(\mathbb{Z}/n\mathbb{Z})^*$ désigne l'indicatrice d'Euler.

1. Soit $F(n) = \{a \in (\mathbb{Z}/n\mathbb{Z})^* \ : \ a^{n-1} = 1\}$.

a) Montrer que $F(n)$ est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$ qui contient $M(n)$.

b) En déduire que si n n'est pas un nombre de Carmichael, alors

$$\mathrm{Card} M(n) \leq \mathrm{Card} F(n) \leq \frac{\varphi(n)}{2}$$

On suppose maintenant que n est un nombre de Carmichael.

2. Soit $I = \left\{ i \in [[0, e]] \ : \ u^{2^i q} = 1 \ \forall u \in (\mathbb{Z}/n\mathbb{Z})^* \right\}$.

a) Montrer que $e \in I$ et que $0 \notin I$.

b) Montrer que si $i \in I \cap [[0, e-1]]$, alors $i + 1 \in I$.

3. Soient $l = \max\{i \in [[0, e-1]] \ : \ i \notin I\}$ et $G = \left\{ u \in (\mathbb{Z}/n\mathbb{Z})^* \ : \ u^{2^l q} \in \{-1, 1\} \right\}$.

a) Montrer que G est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$ qui contient $M(n)$.

b) Montrer qu'il existe un diviseur premier p de n et un entier b premier à n tels que $b^{2^l q} \not\equiv 1 \mod p$.

c) Montrer qu'il existe un entier c tel que $c \equiv b \mod p$ et $c \equiv 1 \mod n/p$.

d) Montrer que $[c]_n \in (\mathbb{Z}/n\mathbb{Z})^* \setminus G$. En déduire que

$$\mathrm{Card} M(n) \leq \mathrm{Card} G \leq \frac{\varphi(n)}{2}$$