université de BORDEAUX	**ANNEE UNIVERSITAIRE 2019/2020** **Examen première session** **Master 1** **Code UE : 4TMA801U, 4TMF801S** **Epreuve : Calcul formel** **Date : 06/05/2020** **Heure : 8h00** **Durée : 10h** Epreuve de M. Jehanne	**Collège Sciences et technologies**

Les fichiers sont à déposer sur moodle et à envoyer à l'adresse `arnaud.jehanne@u-bordeaux.fr`

Il est demandé de rédiger soigneusement et lisiblement. Tous les résultats doivent être justifiés. Compte tenu des circonstances exceptionnelles, **il sera tenu grand compte de la rédaction**.

Vérifiez aussi que vos photos ou scans soient bien lisibles.

Il est interdit de communiquer entre vous et de vous faire aider. Il est permis de consulter le cours et les TD.

Exercice 1 [Bases de Gröbner et systèmes polynomiaux]

Soient dans $\mathbb{Q}[X,Y]$ les polynômes $f_1 = X^2 + Y^2 - 4$ et $f_2 = X^3 + Y^3 - 3XY - 1$.

1. Soit I l'idéal de $\mathbb{Q}[X,Y]$ engendré par f_1 et f_2. En utilisant sage, déterminer la base de Gröbner réduite associée à l'ordre monomial lexicographique $\prec$ tel que $Y \prec X$ et en déduire une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[X,Y]/I$.

2. En utilisant la base de Gröbner de la question **1**, calculer l'ensemble des solutions dans $\mathbb{R}^2$ du système d'équations $f_1(x,y) = f_2(x,y) = 0$.

3. En utilisant sage, faire un graphe représentant les courbes de $\mathbb{R}^2$ d'équation $f_1 = 0$ et $f_2 = 0$, ainsi que leurs points d'intersection.

Exercice 2 [Interpolation d'Hermite]

1. On cherche à trouver un polynôme P de $\mathbb{Q}[x]$ de degré inférieur ou égal à 5 tel que $P(1) = 0$, $P'(1) = -5$, $P''(1) = 10$, $P'''(1) = 60$, $P(2) = 16$ et $P'(2) = 60$.

a) Sur votre copie, traduire ces contraintes en termes de problème de restes chinois (on pourra utiliser le développement de Taylor de P comme indiqué dans le cours).

b) Résoudre le problème en utilisant sage, (par exemple la commande `crt`).

2. Pour tout polynôme P et tout entier naturel i, on note $P^{(i)}$ la dérivée i-ème de P avec la convention : $P^{(0)} = P$.

a) Écrire sur votre fichier sage une fonction `Hermite1` dont les entrées et sorties sont les suivantes.

- Entrée : une liste $l = [a, b]$, où $a \in \mathbb{Q}$ et où b est une liste $[b_0, \ldots, b_r]$ d'éléments de $\mathbb{Q}$.
- Sortie : le polynôme P de degré minimal tel que $P^{(i)}(a) = b_i$ pour tout $i \in [[0, r]]$.

Pour le calcul de $k!$, on peut utiliser la commande `factorial(k)`.

b) Écrire sur votre fichier sage une fonction `Hermite` dont les entrées et sorties sont les suivantes.

- Entrée : une liste $l = [[a_0, b_0], \ldots, [a_s, b_s]]$ où les a_i sont des éléments de $\mathbb{Q}$ et les b_i des listes $[b_{i,0}, \ldots, b_{i,r_i}]$ d'éléments de $\mathbb{Q}$
- Sortie : le polynôme de degré minimal P tel que pour tout $i \in [[0, s]]$ et tout $j \in [[0, r_i]]$,

$$P^{(j)}(a_i) = b_{i,j}$$

Cette fonction utilisera votre fonction `Hermite1` de la question **2. a)** et la fonction `crt`, ou une fonction équivalente de sage.

Exercice 3 [À propos du théorème de Rabin-Miller] On rappelle l'énoncé de ce théorème.

Théorème 1(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, $a^{n-1} \equiv 1 \mod n$. On rappelle 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. Les questions **1**, **2** et **3** ont pour but de démontrer le théorème 2 suivant (nous avons vu un résultat plus fort en cours mais avec une preuve différente, et plus difficile). Dans la question **4** , on montre comment un témoin de non primalité d'un nombre de Carmichaël permet de factoriser ce nombre de Carmichaël.

Théorème 2. *Soit $M(n)$ l'ensemble des faux témoins de primalité pour n de $\mathbb{Z}/n\mathbb{Z}$. Alors*

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

où $\varphi = \text{Card}(\mathbb{Z}/n\mathbb{Z})^*$ 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

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

On suppose maintenant, et jusqu'à la fin de l'exercice, 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 $0 \notin I$ (pour montrer que $0 \notin I$, on pourra essayer $u = -1$).

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

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

4. Soit a un entier premier à n. On suppose que a est un témoin de non primalité pour n. On pose $I_a = \left\{ i \in [[0,e]] \ : \ a^{2^i q} = 1 \ \right\}$.

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

b) Soit $i = \inf I_a$. Montrer que $\text{pgcd}\left(a^{2^{i-1}q} - 1, n\right)$ est un facteur non trivial de n.