université de BORDEAUX	**ANNEE UNIVERSITAIRE 2018/2019** **Examen première session** **Master 1** **Code UE : MSIN820, MSMA820** **Epreuve : Algèbre et calcul formel** **Date : 02/05/2019** **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_Examen.sage`" est à envoyer à l'adresse : `arnaud.jehanne@u-bordeaux.fr`

Il est demandé de rédiger soigneusement et lisiblement. Tous les résultats doivent être justifiés. **En fin d'énoncé sont donnés des rappels sur sage et sur les groupes.**

Exercice 1 [Bases de Gröbner et systèmes polynomiaux]

Dans cet exercice, aucune programmation n'est demandée mais on pourra utiliser sage pour certains calculs. Dans ce cas, il est demandé d'écrire les commandes utilisées et les résultats obtenus sur votre fichier sage ou sws, ou sur votre copie.

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

1. Soit I l'idéal de $\mathbb{Q}[X,Y]$ engendré par f_1 et f_2. En utilisant la base de Gröbner réduite associée à un ordre monomial bien choisi, donner un générateur g de l'idéal $I \cap \mathbb{Q}[Y]$.

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

Exercice 2 [Test de Pocklington-Lehmer]

On rappelle un test de primalité du cours.

Algorithme 1 [Test de Pocklington-Lehmer]

Entrées : n un entier impair et P l'ensemble des facteurs premiers de $n-1$.
Sortie : « n est premier » ou « n est composé »
1. Pour p dans P :
2. $b \leftarrow 1$
3. *Tant que $b = 1$:*
4. *Choisir $a \in [[1, n-1]]$ au hasard*
5. $b \leftarrow$ *reste de la division de $a^{(n-1)/p}$ par n*
6. *Si $b^p \not\equiv 1 \mod n$: sortir « n est composé »*
7. Sortir « n est premier »

1. Programmer sur sage la fonction `TEST1` correspondant à cet algorithme. On pourra tester la fonction sur $n = 10^{10} + 33$. Alors $n - 1 = 2^5 \times 3 \times 11 \times 17 \times 557041$ et $P = [2, 3, 11, 17, 557041]$. L'exécution de `TEST1` ne doit prendre qu'une fraction de seconde.

Pour pouvoir appliquer cette méthode, il faut connaître la factorisation complète de $n-1$. On cherche ici un algorithme similaire qui ne demanderait qu'une factorisation partielle. Pour cela, on va démontrer le résultat suivant.

Théorème 2 *On suppose que $n-1 = FU$ où $pgcd(F,U) = 1$ et $U > 1$. On suppose aussi que tous les diviseurs premiers de U sont strictement supérieurs à un entier B tel que $BF \geq \sqrt{n}$. Alors n est premier si et seulement si les conditions suivantes sont vérifiées.*

(i) Pour tout diviseur premier p de F, il existe un entier a_p tel que $a_p^{n-1} \equiv 1 \mod n$ et $pgcd\left(a_p^{(n-1)/p} - 1, n\right) = 1$

(ii) Il existe un entier a tel que $a^{n-1} \equiv 1 \mod n$ et $pgcd\left(a^F - 1, n\right) = 1$

2. On suppose que n est un nombre premier. Expliquer pourquoi les conditions (i) et (ii) du théorème sont vérifiées (on pourra considérer un entier g tel que $[g]_n$ engendre $(\mathbb{Z}/n\mathbb{Z})^*$ et choisir $a = g$ et $a_p = g$ pour tout p).

Réciproquement, on suppose que (i) et (ii) sont vérifiées. On veut montrer que n est premier. **Soit l le plus petit nombre premier qui divise n.**

3. a) Soit P_F l'ensemble des nombres premiers qui divisent F et soit $F = \prod_{p \in P_F} p^{v_p}$ la factorisation complète de F. Soit $p \in P_F$, montrer que p^{v_p} divise $l - 1$ (on pourra par exemple considérer l'ordre de $[a_p]_l^{(n-1)/p^{v_p}} \in (\mathbb{Z}/l\mathbb{Z})^*$).

b) En déduire que F divise $l - 1$.

4. a) On note ω l'ordre de $[a]_l$ dans $(\mathbb{Z}/l\mathbb{Z})^*$. Montrer que ω divise $n - 1$ et que ω ne divise pas F.

b) En déduire que $\text{pgcd}(\omega, U) \neq 1$. Soit t un nombre premier divisant $\text{pgcd}(\omega, U)$.

c) Montrer que t divise $l - 1$.

5. Montrer que tF divise $l - 1$.

6. Montrer que $l > \sqrt{n}$ et terminer la preuve du théorème.

7. Programmer la fonction `TEST2` suggérée par le théorème 2. Cette fonction prendra en entrées l'entier n, le facteur F et une liste P de nombres premiers tels que F se factorise complètement sur P. En sortie, elle rendra « n est premier » ou « n est composé ». On pourra tester cette fonction sur l'exemple de la question 8 suivante (ce calcul ne doit prendre qu'une fraction de seconde).

8. Soit $n = 10^{20} + 207$. On suppose qu'après division de n par tous les nombres premiers inférieurs à 1532, on a trouvé que $n - 1 = FU$ où $F = 2 \times 3^2 \times 811 \times 1531$ et où tous les facteurs premiers de U sont supérieurs à 1532. Vérifier que $\texttt{TEST2}(n, F, [2, 3, 811, 1531])$ permet de montrer que n est premier (on pourra utiliser sage et décrire sur papier les calculs qui permettent de conclure).

Exercice 3 [Facteurs irréductibles des polynômes cyclotomiques dans $\mathbb{F}_q[X]$]

Soit $n \geq 1$ un entier. Pour tout corps K, on note $\text{Prim}(K, n)$ l'ensemble des racines primitives n-èmes de 1 appartenant à K. Soit

$$\Phi_n = \prod_{\omega \in \text{Prim}(\mathbb{C}, n)} (X - \omega)$$

le n-ème polynôme cyclotomique de $\mathbb{C}[X]$. On rappelle que pour tout entier n, Φ_n est un polynôme irréductible de $\mathbb{Z}[X]$.

Soient p un nombre premier qui ne divise pas n et $\mathbb{F}_p^c$ une clôture algébrique de $\mathbb{F}_p$. On s'intéresse ici à la réduction modulo p de Φ_n. On la note $[\Phi_n]_p \in \mathbb{F}_p[X]$. On rappelle aussi (ou on admet) que

$$[\Phi_n]_p = \prod_{\omega \in \text{Prim}(\mathbb{F}_p^c, n)} (X - \omega)$$

Pour toute puissance q de p, on note $\mathbb{F}_q$ le corps de cardinal q inclus dans $\mathbb{F}_p^c$. Soit q une puissance de p fixée. Tous les polynômes sont maintenant considérés dans $\mathbb{F}_q[X]$. **Pour alléger les notations, on note Φ_n à la place de $[\Phi_n]_p$** (le polynôme Φ_n est maintenant considéré comme un polynôme de $\mathbb{F}_p[X] \subset \mathbb{F}_q[X]$). **Soit d l'ordre de $[q]_n$ dans $(\mathbb{Z}/n\mathbb{Z})^*$.**

1. Nous allons démontrer dans les questions 2 et 3 que dans $\mathbb{F}_q[X]$, tous les facteurs irréductibles du polynôme cyclotomique Φ_n ont même degré d (défini ci-dessus).

En admettant ce fait, en déduire le degré des facteurs irréductibles de Φ_{16} dans $\mathbb{F}_3[X]$ (ceci sans calculer la factorisation, mais plutôt en calculant 3^2 et 3^4 modulo 16).

2. Soit f un facteur irréductible de Φ_n et soit α une racine de f dans $\mathbb{F}_p^c$ (donc $\mathbb{F}_q[\alpha] \simeq \mathbb{F}_q[X]/(f)$). Soit enfin $d' = \deg f$.

a) Justifier pourquoi α est un élément d'ordre n de $\mathbb{F}_q[\alpha]^*$, puis montrer que $q^{d'} \equiv 1 \mod n$.

b) En déduire que d divise d'.

3. Montrer que $\alpha \in \mathbb{F}_{q^d}$. En déduire que $\mathbb{F}_q[\alpha] \subset \mathbb{F}_{q^d}$ et que d' divise d.

Remarque. Cet exercice montre que si l'on veut factoriser Φ_n dans $\mathbb{F}_q[X]$, on peut lui appliquer directement l'algorithme de Cantor-Zassenhaus.

Rappels

• Quelques commandes sage

— Pour définir l'anneau `Qxy`$= \mathbb{Q}[x, y]$:

```
Qxy.<x,y>=PolynomialRing(QQ,order='ordre choisi')
```

où l'ordre choisi $\prec$ est l'un des ordres suivants vérifiant $x \succ y$.

`'degrevlex'` (ordre par défaut) - ordre lexicographique gradué inverse

`'lex'` - ordre lexicographique

`'deglex'` - ordre lexicographique gradué

— Pour définir l'idéal I de $\mathbb{Q}[x, y]$ engendré par une liste l de polynômes : `I=ideal(l)`. Sa base de Gröbner peut être calculée grâce à la commande `I.groebner_basis()`.

• Ordre d'un élément dans un groupe

Soit G un groupe. Soient $g \in G$ et $n \in \mathbb{N} \setminus \{0\}$. On dit que g est d'ordre n si $g^n = 1$ et si n est le plus petit entier strictement positif vérifiant cette propriété.

On rappelle ci-dessous quelques résultats à ce sujet.

— Si g est d'ordre n et si G est fini, n divise $\mathrm{card}(G)$.

— On suppose que g est d'ordre n. Alors $g^k = 1$ si et seulement si n divise k.

— g est d'ordre n si et seulement si les propriétés suivantes sont vérifiées.

(i) $g^n = 1$

(ii) pour tout diviseur d de n distinct de n, $g^d \neq 1$

— g est d'ordre n si et seulement si les propriétés suivantes sont vérifiées.

(i) $g^n = 1$

(ii) pour tout diviseur premier p de n, $g^{n/p} \neq 1$

— Soit G un groupe cyclique de cardinal n. Soit d un diviseur de n. Alors

$$H = \{g \in G \ : \ g^d = 1\}$$

est l'unique sous-groupe de G de cardinal d.