université de BORDEAUX	**ANNEE UNIVERSITAIRE 2018/2019** **Examen première session** **Master 1** **Code UE : MSIN820, MSMA820** **Epreuve : Algèbre et calcul formel** **Date : 2/05/2019** **Heure : 9h00** **Durée : 3h** **Corrigé**	**Collège Sciences et technologies**

Exercice 1 [Bases de Gröbner et systèmes polynomiaux]

1. Comme on veut faire de l'élimination, on choisit l'ordre lexicographique. On trouve la base de Gröbner réduite $G = (g_0, g_1, g_2)$ où $g_0 = X^2 + Y^2 - 4$, $g_1 = Y(X + Y^3 + Y^2 - 3Y - 2)$, et $g_3 = Y^2(Y+2)(Y^2-2)$. Comme on a choisi l'ordre lexicographique, on a vu que $G \cap \mathbb{Q}[Y]$ engendre $I \cap \mathbb{Q}[Y]$. Ainsi, $I \cap \mathbb{Q}[Y] = Y^2(Y+2)(Y^2-2)$.
2. Le système $f_1(x,y) = f_2(x,y) = 0$. est équivalent au système $g_0(x,y) = g_1(x,y) = g_2(x,y) = 0$. La factorisation de g_2 montre que pour toute solution (x,y), $y \in \{0, -2, \sqrt{2}, -\sqrt{2}\}$. On vérifie que $(2,0)$ et $(-2,0)$ sont solutions telles que $y = 0$. On continue ainsi et on trouve comme ensemble de solutions $\mathcal{S}ol = \{(-2,0), (2,0), (0,-2), (\sqrt{2},\sqrt{2}), (-\sqrt{2},-\sqrt{2})\}$.

Exercice 2 [Test de Pocklington-Lehmer]
1. Voir le fichier sage.
2. Comme n est premier, le groupe $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ est cyclique d'ordre $n-1$. Soit g un entier tel que $[g]_p$ engendre ce groupe. Alors pour tout nombre premier p divisant $n-1$, $g^{n-1} \equiv 1 \mod n$ et $g^{(n-1)/p} \not\equiv 1 \mod n$. Ce dernier fait signifie que n ne divise pas $g^{(n-1)/p} - 1$, c'est-à-dire que $\text{pgcd}(n, g^{(n-1)/p} - 1) = 1$ puisque n est premier.

De même, comme F divise $n-1$ et $F \neq n-1$, $g^F \not\equiv 1 \mod n$ et donc $\text{pgcd}(n, g^F - 1) = 1$.
3. a) Soit $x = [a_p]_l^{(n-1)/p^{v_p}} \in (\mathbb{Z}/l\mathbb{Z})^*)$. Alors $x^{p^{v_p}} = 1$ et $x^{p^{v_p-1}} \neq 1$. On en déduit que l'ordre de x est égal à p^{v_p} et donc que p^{v_p} divise $l-1$ puisque $l-1 = |(\mathbb{Z}/l\mathbb{Z})^*|$.

b) Soit $\mathcal{F}$ l'ensemble des nombres premiers qui divisent F. Donc $F = \prod_{p\in\mathcal{F}} p^{v_p}$. Comme pour tout $p \in \mathcal{F}$, p^{v_p} divise $l-1$, $F = \text{ppcm}\{p^{v_p} \ : \ p \in \mathcal{F}\}$ divise $l-1$.
4. a) Comme $[a]_l^{n-1} = 1$, c'est que l'ordre ω de $[a]_l$ divise $n-1$. Comme $\text{pgcd}(a^F - 1, n) = 1$, l ne divise pas $a^F - 1$ donc $[a]_l^F \neq 1$, ce qui montre que ω ne divise pas F.

b) Supposons par l'absurde que $\text{pgcd}(\omega, U) \neq 1$. Comme $FU = n-1$, ω divise FU. donc ω divise F (puisqu'il est supposé premier à U). C'est absurde d'après la question précédente.

c) Comme t divise ω et ω divise $n-1$, on déduit que t divise $l-1$.
5. Comme t et F divisent $l-1$ et sont premiers entre eux, tF divise $l-1$.
6. Comme t divise U, $t \geq B$ donc $\sqrt{n} \leq BF \leq tF \leq l-1 < l$. Comme l est le plus petit nombre premier qui divise n, on en déduit que $n = l$ est premier.
7. Voir le fichier sage.
8. Soit $n = 10^{20} + 207$. On calcule $F = 2 \times 3^2 \times 811 \times 1531 = 22349538$. Un autre calcul sur sage montre que $(1532 \times F)^2 - n > 0$. L'entier F vérifie donc bien les hypothèses du théorème et on peut appliquer `TEST2`. Ce test montre que n est premier.

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

1. $3^2 \equiv 9 \not\equiv 1 \mod 16$ et $3^4 \equiv 1 \mod 16$) donc $[3]_{16}$ est d'ordre 4 : les facteurs irréductibles de Φ_{16} sont de degré 4. Il y en a donc $\varphi(16)/4 = 2$. On vérifie sur sage : dans $\mathbb{F}_3[X]$,

$$\Phi_{16} = (X^4 + X^2 + 2)(X^4 + 2X^2 + 2)$$

2. a) α est une racine de f, donc de Φ_n. Cela veut dire que α est d'ordre n. Comme $\alpha \in \mathbb{F}_q[\alpha]^*$, on en déduit que n divise $\mathrm{Card}(\mathbb{F}_q[\alpha]^*) = q^{d'} - 1$ donc que $q^{d'} \equiv 1 \mod n$.

b) Comme d est l'ordre de $[q]_n$, on en déduit que d divise d'.

3. Comme d est l'ordre multipicatif de $[q]_n$, il existe k dans $\mathbb{Z}$ tel que $q^d = 1 + kn$, donc

$$\alpha^{q^d} = \alpha^{1+kn} = \alpha\alpha^{kn} = \alpha$$

puisque $\alpha^n = 1$. Cela montre que $\alpha \in \mathbb{F}_{q^d}$ et donc $\mathbb{F}_q[\alpha] \subset \mathbb{F}_{q^d}$. Comme $\mathbb{F}_q[\alpha] = \mathbb{F}_{q^{d'}}$, on en déduit que d' divise d.