	ANNEE UNIVERSITAIRE 2016/2017 **Examen première session** **Master 1** **Code UE : MSIN820, MSMA820** **Epreuve : Algèbre et calcul formel** **Date : 3/05/2017** **Heure : 9h00** **Durée : 3h** Documents autorisés : Feuilles d'exercices (énoncés). Epreuve de M. Jehanne	**Collège Sciences et technologies**

Corrigé

Exercice 1 [Factorisation dans $\mathbb{N}$: la méthode de Fermat]

Pour factoriser un entier n, la méthode de Fermat consiste à chercher à l'écrire sous la forme

$$n = x^2 - y^2 = (x+y)(x-y). \tag{1}$$

La méthode est la suivante. On pose $u = \lceil \sqrt{n} \rceil$ (le plus petit entier supérieur ou égal à $\sqrt{n}$) et $v = u^2 - n$. Si v est un carré, alors $x = u$ et $y = \sqrt{v}$ vérifient (1). Si tel n'est pas le cas, on essaie avec l'entier suivant $u' = u + 1$ et $v' = u'^2 - n$. Si v' est un carré, on termine comme ci-dessus. Sinon, on remplace u par u' et v par v', puis on itère le procédé.

1. *Montrer que $v' = v + 2u + 1$ (cela permet un calcul plus rapide de v').*

$$v' = u'^2 - n = (u+1)^2 - n = u^2 - n + 2u + 1 = v + 2u + 1$$

2. *Programmer une fonction* `Fermat` *correspondant à cette méthode. On y insérera un test permettant de stopper l'exécution dès que 10^6 valeurs de u ont été calculées.*

Cette fonction prendra en entrée un entier naturel n et donnera en sortie un facteur non trivial de n, ou bien `Echec` *dans le cas où les 10^6 calculs de u auront été atteints.*

On pourra tester `Fermat` *sur les entiers* 13199, $\dfrac{10^{22}+1}{89.101}$ *(pour ces deux entiers, le calcul doit aboutir rapidement),* $7.10^{10} + 133$ *et* $10^{20} + 67$ *(c'est normal si ça ne donne rien).*

Exercice 2 [Irréductibilité dans $\mathbb{F}_p[x]$] *Soit p un nombre premier On cherche à construire des polynômes irréductibles dans $\mathbb{F}_p[x]$ de degré donné.*

Théorème. *Pour tout entier $n \geq 1$, le polynôme $x^{p^n} - x \in \mathbb{F}_p[x]$ est le produit des polynômes irréductibles unitaires de $\mathbb{F}_p[x]$ dont le degré divise n.*

En utilisant ce théorème, nous avons vu en cours un algorithme qui teste si un polynôme de $\mathbb{F}_p[x]$ est irréductible ou non.

Algorithme `EstIrreductible`.
Entrées : un nombre premier p, un entier $n > 1$, un polynôme $f \in \mathbb{F}_p[x]$ de degré n et l'ensemble $\mathcal{P}$ des diviseurs premiers de n.
Sortie : `true` *si f est irréductible,* `false` *sinon.*

1. *Calculer le reste a de la division de x^{p^n} par f*
2. *Si $a \neq x$ sortir* `false`
3. *Pour tout $t \in \mathcal{P}$*
4. *Calculer le reste b de la division de $x^{p^{n/t}}$ par f*
5. *Si* $\text{pgcd}(b - x, f) \neq 1$, *sortir* `false`
6. *Sortir* `true`

1. *Programmer* `EstIrreductible` *sur sage en s'efforçant d'obtenir la meilleure complexité possible. On pourra tester la fonction sur les polynômes x^6+x+1 et $x^6+x+2 \in \mathbb{F}_{11}[x]$ puis $x^{601}-x-1$ et $x^{600} - x - 1 \in \mathbb{F}_{601}[x]$ (cela ne doit prendre que quelques secondes).*

2. *On se donne un entier naturel n non nul et on veut trouver un polynôme irréductible $f \in \mathbb{F}_p[x]$ unitaire de degré n. Pour cela, on choisit au hasard un polynôme $g \in \mathbb{F}_p[x]$ tel que $\deg g < n$ et on utilise* `EstIrreductible` *pour tester l'irréductibilité de $f = x^n + g$. On recommence jusqu'à trouver un polynôme f irréductible.*

En utilisant cette méthode, écrire une fonction `Irreductible` *qui en entrée prend un nombre premier p et un entier naturel non nul n et qui en sortie rend un polynôme irréductible unitaire de degré n dans $\mathbb{F}_p[x]$.* **3.** *On veut évaluer le nombre moyen de tirages nécessaire à l'exécution de la fonction* `Irreductible`*. Soient $I(n)$ l'ensemble des polynômes unitaires irréductibles de degré n de $\mathbb{F}_p[x]$ et $f_n = \prod_{f \in I(n)} f$.* **a.** *Montrer que $n\mathrm{Card}I(n) \leq p^n$.*

On utilise le théorème cité dans l'énoncé. Avec les notations données, il s'écrit

$$x^{p^n} - x = \prod_{d|n} f_d.$$

En prenant les degrés, on obtient

$$p^n = \sum_{d|n} \deg f_d = \sum d\mathrm{Card}I(d)$$

donc $p^n \geq n\mathrm{Card}I(n)$.

b. *Montrer les inégalités*

$$\sum_{d|n, d\neq n} \deg f_d \leq \frac{p(p^{\frac{n}{2}} - 1)}{p-1} \leq 2p^{\frac{n}{2}} \quad \textit{et} \quad n\mathrm{Card}I(n) \geq p^n - 2p^{\frac{n}{2}}.$$

$$\begin{aligned}
\sum_{d|n, d\neq n} \deg f_d &\leq \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} \deg f_d \\
&\leq \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} p^d \\
&\leq \frac{p(p^{\lfloor \frac{n}{2} \rfloor} - 1)}{p-1} \\
&\leq \frac{p(p^{\frac{n}{2}} - 1)}{p-1} \\
&\leq 2p^{\frac{n}{2}}
\end{aligned}$$

puisque $\dfrac{p}{p-1} \leq 2$ dès que $p \geq 2$. La seconde inégalité en découle :

$$n\mathrm{Card}I(n) = p^n - \sum_{d|n, d\neq n} \deg f_d \geq p^n - 2p^{\frac{n}{2}}.$$

c. *Soit P_n la probabilité d'obtenir un polynôme irréductible f après un tirage effectué dans la fonction* `Irreductible`*. Montrer que*

$$\frac{1}{n}\left(1 - \frac{2}{p^{\frac{n}{2}}}\right) \leq P_n \leq \frac{1}{n}.$$

Comme la probabilité est uniforme, $P_n = \dfrac{\mathrm{Card}I(n)}{\mathrm{Card}\mathbb{F}_p[x]_{n-1}} = \dfrac{\mathrm{Card}I(n)}{p^n}$, ce qui prouve les inégalités demandées grâce à la question précédente.

d. *On suppose que* $p^n \geq 16$. *Montrer que* $\frac{1}{2n} \leq P_n \leq \frac{1}{n}$. *Soient* T_n *le nombre de tirages et* $E(T_n)$ *l'espérance de* T_n. *Montrer que* $n \leq E(T_n) \leq 2n$.

Il est facile de voir que si $p^n \geq 16$, alors $1 - \frac{2}{p^{\frac{n}{2}}} \geq \frac{1}{2}$ donc $\frac{1}{2n} \leq P_n \leq \frac{1}{n}$.

$$E(T_n) = \sum_{k=1}^{+\infty} P(T_n = k) = P_n \sum_{k=1}^{+\infty} (1 - P_n)^{k-1}.$$

La somme est égale à la dérivée de la fonction $x \mapsto \frac{1}{1-x}$ prise en $x = 1 - P_n$. On en déduit que $E(T_n) = \frac{1}{P_n}$ donc $n \leq E(T_n) \leq 2n$.

Exercice 3 [Bases de Gröbner] *Dans cet exercice, aucune programmation n'est demandée mais on pourra utiliser sage pour certains calculs. Dans ce cas, il vous est demandé d'écrire les commandes utilisées et les résultats obtenus sur votre fichier sage ou sws, ou sur votre copie.*

On s'intéresse à la résolution de systèmes d'équations polynomiales. La partie 1 utilise une méthode vue en cours et en TD. Les parties 2 et 3 abordent une autre méthode.

1. *Soient dans* $\mathbb{Q}[X, Y]$ *les polynômes*

$$f_1 = X^2 + Y^2 - 4 \quad et \quad f_2 = XY + X - Y - 2$$

a. *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* $I \cap \mathbb{Q}[Y]$.

On choisit l'ordre lexicographique $\succ$ tel que $x \succ y$. Alors si $\mathcal{G}$ est une base de Gröbner de I, $\mathcal{G} \cap \mathbb{Q}[Y]$ est une base de Gröbner de $I \cap \mathbb{Q}[Y]$. Pour cela, on peut utiliser les commandes suivantes.

```
QXY.<X,Y>=PolynomialRing(QQ,order='lex')
f1=X**2+Y**2-4
f2=X*Y+X-Y-2
I=QXY.ideal([f1,f2])
I.groebner()
```

On obtient la base de Gröbner (g_0, g_1) où $g_0 = X + Y^3 + Y^2 - 3Y - 2$ et $g_1 = Y^4 + 2Y^3 - 2Y^2 - 4Y = Y(Y + 2)(Y^2 - 2)$. On conclut que

$$I \cap \mathbb{Q}[Y] = y(Y + 2)(Y^2 - 2)\mathbb{Q}[Y].$$

b. *En déduire l'ensemble des solutions dans* $\mathbb{C}^2$ *du système d'équations* $f_1(x, y) = f_2(x, y) = 0$.

Soit (x, y) une solution. Alors $g_1(y) = 0$ donc $y \in \{0, -2, \sqrt{2}, -\sqrt{2}\}$. Comme $g_0(x, y) = 0$, c'est que $x = -y^3 - y^2 + 3y + 2$. L'ensemble des solutions est donc

$$\mathcal{S} = \{(0, 2), (-2, 0), (\sqrt{2}, \sqrt{2}), (-\sqrt{2}, -\sqrt{2})\}.$$

2. *Soit* K *un corps quelconque. On pose* $X = (X_1, \ldots, X_n)$ *et on considère l'anneau des polynômes à plusieurs variables* $K[X] = K[X_1, \ldots, X_n]$. *Nous proposons ici une autre méthode pour la résolution de systèmes d'équations polynomiales.*

Soient $f_1, \ldots, f_s \in K[X]$ *et* I *l'idéal de* $K[X]$ *engendré par* $f_1, \ldots, f_s$. *On suppose que le* K*-espace vectoriel* $K[X]/I$ *est de dimension finie. Pour tout polynôme* f *de* $K[X]$, *on note* $[f]$ *la classe de* f *dans* $K[X]/I$. *Pour tout* $P \in K[X]$, *on définit l'application*

$$\begin{aligned} m_P \ : \ K[X]/I &\to K[X]/I \\ [f] &\mapsto [Pf] \end{aligned}$$

a. *Montrer que m_P est un endomorphisme du K-espace vectoriel $K[X]/I$.*

Laissé au lecteur.

b. *Soient $b_1, \dots, b_d \in K[X]$ tels que $\mathcal{B} = ([b_1], \dots, [b_d])$ est une base de $K[X]/I$. On note A_P la matrice de m_P dans la base $\mathcal{B}$. Autrement dit, si l'on note $(a_{ij})_{(i,j)\in[[,1,d]]^2}$ les coefficients de A_P,*

$$m_P([b_j]) = \sum_{i=1}^{d} a_{ij}[b_i].$$

Soit L un corps contenant K et $x \in L^n$ tel que $f_1(x) = \cdots = f_s(x) = 0$. Montrer que le vecteur colonne ${}^t(b_1(x), \dots, b_d(x))$ est vecteur propre de ${}^tA_P$ pour la valeur propre $P(x)$.

Soit $c(x) = {}^tA_P{}^t(b_1(x)\dots, b_d(x))$. On note $c(x)_j$ sa j-ème coordonnée.

$$c(x)_j = \sum_{i=1}^{d} a_{ij} b_i(x).$$

L'égalité

$$m_P([b_j]) = \sum_{i=1}^{d} a_{ij}[b_i]$$

signifie qu'il existe un polynôme $F \in I$ tel que

$$Pb_j = \sum_{i=1}^{d} a_{ij} b_i + F.$$

Comme $F(x) = 0$, on en déduit

$$P(x)b_j(x) = \sum_{i=1}^{d} a_{ij} b_i(x) = c(x)_j$$

ce qu'il fallait démontrer.

c. *En déduire une méthode algorithmique pour la résolution du système polynomial*

$$f_1(x) = \cdots = f_s(x) = 0$$

(en cas de doute, on pourra laisser un blanc et revenir à cette question après la partie 3 suivante).

Pour tout $i \in [[1, n]]$, on peut calculer l'ensemble $\mathcal{V}_i$ des valeurs propres de la matrice A_{X_i} correspondant au polynôme X_i puis on teste tous les éléments de $\prod_{i=1}^{n} \mathcal{V}_i$.

3. *On reprend l'exemple de la question 1. On considère donc l'anneau $\mathbb{Q}[X, Y]$ et l'idéal I engendré par les polynômes $f_1 = X^2 + Y^2 - 4 \quad et \quad f_2 = XY + X - Y - 2$.*

On munit $\mathbb{Q}[X, Y]$ de l'ordre monomial lexicographique gradué $\succeq$ avec $X \succeq Y$. Dans sage, cet ordre est appelé `deglex`.

a. *Calculer la base de Gröbner réduite de l'idéal I. En déduire une base $\mathcal{B}$ du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[X, Y]/I$.*

On exécute les commandes suivantes.

```
QXY.<X,Y>=PolynomialRing(QQ,order='deglex')
f1=X**2+Y**2-4
f2=X*Y+X-Y-2
I=QXY.ideal([f1,f2])
I.groebner()
```

On obtient la base de Gröbner (h_0, h_1, h_2) où $h_0 = g_0 = Y^3 + Y^2 + X - 3Y - 2$, $h_1 = f_1 = X^2 + Y^2 - 4$ et $h_2 = f_2 = XY + X - Y - 2$. Les termes dominants sont $\mathrm{lt}(h_0) = Y^3$, $\mathrm{lt}(h_1) = X^2$ et $\mathrm{lt}(h_2) = XY$. L'ensemble de monômes standards de $\mathbb{Q}[X,Y]/I$ pour l'ordre lexicographique gradué est $\{1, X, Y, Y^2\}$. $\mathcal{B} = ([1], [X], [Y], [Y^2])$ est une base de $\mathbb{Q}[X,Y]/I$.

b. *Calculer les matrices A_X et A_Y de m_X et m_Y dans la base $\mathcal{B}$ et leurs valeurs propres.*

On peut calculer ces matrices à la main ou utiliser sage. Pour cela, on définit le quotient $\mathbb{Q}[X,Y]/I$ dans sage et calculer les produits nécessaires dans ce quotient.

```
QXYsurI.<a,b>=QXY.quotient(I)
```

Alors $a = [X]$ et $b = [Y]$.

Comme $X.1 = X$, la première colonne de A_X est ${}^t(0,1,0,0)$. Puis on calcule X^2 grâce à la commande `a**2` qui donne `-b**2+4` (ce qui peut aussi se voir sur le polynôme f_1). Donc la seconde colonne est ${}^t(4,0,0,-1)$. On continue ainsi et on trouve

$$A_X = \begin{pmatrix} 0 & 4 & 2 & -2 \\ 1 & 0 & -1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & -1 & 0 & 1 \end{pmatrix} \quad \text{et} \quad A_Y = \begin{pmatrix} 0 & 2 & 0 & 2 \\ 0 & -1 & 0 & -1 \\ 1 & 1 & 0 & 3 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

dont les polynômes caractéristiques respectifs sont

$$\chi_X(t) = t(t-2)(t^2-2) \quad \text{et} \quad \chi_Y(t) = t(t+2)(t^2-2)$$

c. *En déduire l'ensemble des solutions dans $\mathbb{C}^2$ du système $f_1(x,y) = f_2(x,y) = 0$.*

D'après la question précédente, si (x,y) est une solution du système,

$$(x,y) \in \{0, 2, \sqrt{2}, -\sqrt{2}\} \times \{0, -2, \sqrt{2}, -\sqrt{2}\}.$$

En testant chacun des éléments de cet ensemble, on obtient

$$\mathcal{S} = \{(0,-2), (2,0), (\sqrt{2}, \sqrt{2}), (-\sqrt{2}, -\sqrt{2})\}.$$