Université Bordeaux 1 — **MHT839 – Master**
Mathématiques — Année 2013–2014

Devoir Surveillé, 16 avril 2014
Durée 2h.

Quelques commandes sage sont rappelées en annexe. Pour les commandes liées aux polynômes multivariés, se reporter à la feuille d'exercices 14.

Exercice 1 – [Polynômes multivariés]
En utilisant une base de Gröbner (calculée à l'aide de sage), déterminer l'ensemble des $(x, y) \in \mathbb{R}^2$ tels que

$$\begin{cases} x^3 + y^3 - 3xy = 1 \\ x^2 + y^2 = 4 \end{cases}$$

Indiquez sur votre copie l'ordre sur les monômes utilisé, la base de Gröbner obtenue, et le raisonnement qui s'ensuit.

Exercice 2 – [Factorisation sur $\mathbb{F}_2[x]$]
Dans cet exercice, on se propose de programmer une version de l'algorithme de Cantor-Zassenhaus adaptée à $\mathbb{F}_2[x]$. À toute fin utile, l'algorithme de Cantor-Zassenhaus en caractéristique impaire est rappelé en annexe. Soit m un entier naturel non nul. Soit

$$T_m(x) = x^{2^{m-1}} + \cdots + x^2 + x \in \mathbb{F}_2[x].$$

Ce polynôme induit l'application t_m de $\mathbb{F}_{2^m}[x]$ dans lui-même qui à $a \in \mathbb{F}_{2^m}[x]$ associe $T_m(a)$. On rappelle que t_m est linéaire, que $\operatorname{Im} t_m = \mathbb{F}_2$ et que $\#\operatorname{Ker} t_m = \#t_m^{-1}(1) = 2^{m-1}$.

Pour tout entier naturel non nul, on note $\mathcal{P}(d)$ l'ensemble des produits de polynômes irréductibles deux à deux distincts de degré d. Soit $Q \in \mathcal{P}(d)$ non irréductible de degré n et soient $P_1, \ldots, P_r$ les facteurs irréductibles de Q. Pour tout i, on note φ_i la surjection canonique de $\mathbb{F}_2[x]$ dans $\mathbb{F}_2[x]/(P_i)$.

1) (sur papier) Soient $A \in \mathbb{F}_2[x]$ et $I_A = \{i \in [[1, r]] \ : \ T_d(\varphi_i(A)) = 0\}$. Montrer :

$$\operatorname{pgcd}(T_d(A), Q) = \prod_{i \in I_A} P_i.$$

2) (sur papier) En déduire que si A est choisi au hasard dans $\{f \in \mathbb{F}_2[x] \ : \ \deg f < n\}$ avec une loi de probabilité uniforme, alors $\operatorname{pgcd}(T_d(A), Q)$ est un diviseur non trivial de Q avec une probabilité $1 - 2^{1-r}$.

3) (sur machine) En utilisant les résultats précédents, écrire une fonction qui, étant donné un polynôme $Q \in \mathcal{P}(d)$ non irréductible, rend un facteur non trivial de Q avec une probabilité supérieure à $1/2$ (les variables de la fonction sont donc Q et d).

Pour tester votre fonction, vous pourrez prendre par exemple $Q = (x^{64} + x + 1)/(x^4 + x + 1)$ et $d = 12$.

Exercice 3 – [Relation de Bézout à n termes]

1) (sur papier) Soient a_0, a_1, a_2 trois entiers. On note $d_1 = \mathrm{pgcd}(a_0, a_1)$ et $d_2 = \mathrm{pgcd}(d_1, a_2) = \mathrm{pgcd}(a_0, a_1, a_2)$. Soient v_0, v_1, w_1 et w_2 des entiers tels que $v_0 a_0 + v_1 a_1 = d_1$ et $w_1 d_1 + w_2 a_2 = d_2$. Déterminer des entiers u_0, u_1 et u_2 tels que $u_0 a_0 + u_1 a_1 + u_2 a_2 = d_2$.

2) (sur machine) Soit $n \geqslant 1$ un entier. Écrire une fonction qui, étant donnée une liste $[a_0, \ldots, a_{n-1}]$ de n entiers, calcule $d = \mathrm{pgcd}(a_0, \ldots, a_{n-1})$ et une liste $[u_0, \ldots, u_{n-1}]$ telle que

$$d = \sum_{i=0}^{n-1} u_i a_i.$$

On pourra utiliser la commande `xgcd(a,b)`, qui rend un triplet (d, u, v) tel que $\mathrm{pgcd}(a, b) = d$ et $au + bv = d$. Pour tester votre fonction, vous pouvez prendre par exemple $a = [42, 70, 105]$, ou bien $[42, 70, 105, 75]$.

3) (sur papier) Soient a et b deux entiers, $d = \mathrm{pgcd}(a, b)$ et soient u et v deux entiers tels que $au + bv = d$. Vérifier que la matrice $U = \begin{pmatrix} u & -b/d \\ v & a/d \end{pmatrix}$ est une matrice de $\mathrm{GL}_2(\mathbb{Z})$ telle que $(a, b)U = (d, 0)$.

4) (sur machine) Écrire une fonction qui, étant donné un vecteur $a = (a_0, \ldots, a_{n-1})$ de n entiers, calcule $d = \mathrm{pgcd}(a_0, \ldots, a_{n-1})$ et une matrice $U \in \mathrm{GL}_n(\mathbb{Z})$ telle que $(a_0, \ldots, a_{n-1})U = (d, 0, \ldots, 0)$.

Indication : au début, on pose $U = I_n$ en écrivant `U=matrix.identity(n)`. *Supposons qu'à l'étape i on ait obtenu une matrice U telle que*

$$aU = (d_{i-1}, 0, \ldots, 0, a_i, \ldots, a_{n-1}),$$

où $d_i = \mathrm{pgcd}(a_0, \ldots, a_{i-1})$. S'inspirant de la question précédente, on définit une matrice M en écrivant d'abord `M=matrix.identity(n)`, *puis en modifiant les coordonnées $m_{0,0}$, $m_{0,i}$, $m_{i,0}$, $m_{i,i}$ de M de telle sorte que $M \in GL_n(\mathbb{Z})$ et que*

$$(d_{i-1}, 0, \ldots, 0, a_i, \ldots, a_{n-1})M = (d_i, 0, \ldots, 0, a_{i+1}, \ldots, a_{n-1}),$$

où $d_i = \mathrm{pgcd}(d_{i-1}, a_i)$. Faire alors $U \longleftarrow UM$.

5) (sur papier) Expliquer comment résoudre dans $\mathbb{Z}$ une équation $\sum_{i=0}^{n-1} a_i x_i = b$, où les a_i et b appartiennent à $\mathbb{Z}$ (on pourra exprimer cette équation sous forme matricielle, puis insérer une matrice $I_n = UU^{-1}$).

6) (sur papier, en utilisant la machine) En utilisant cette méthode, résoudre l'équation $54x+165y+100z = 1$ (indiquer les résultats intermédiaires, notamment la matrice U obtenue).

Quelques commandes sage.

Les commandes suivantes pourront vous être utiles. Pas forcément toutes. Cela dépend des méthodes que vous choisirez.

Entiers et polynômes

`k=GF(p)` (pour définir le corps fini $\mathbb{F}_p$).
`pr.<x>=PolynomialRing(k)` (pour l'anneau $k[x]$).
Pour choisir un élément au hasard dans un ensemble E préalablement défini : `E.random_element()`
Par exemple, pour choisir un polynôme au hasard de degré inférieur ou égal à n dans `pr`$= k[x]$: `pr.random_element(n)`
`gcd(P,Q)` : $\mathrm{pgcd}(P, Q)$.
`P.degree()` : $\deg P$ (si P est dans un anneau `pr`$= k[x]$ comme ci-dessus).
Pour le quotient de a par $b \neq 0$: `a//b` (où a et b sont des entiers ou des polynômes).
Pour le reste de a par $b \neq 0$: `a%b` (où a et b sont des entiers ou des polynômes).
Pour le quotient et le reste de P par $Q \neq 0$ (dans `pr`$= k[x]$) : `P.quo_rem(Q)`.
Pour se placer dans un anneau quotient $k[x]/(P)$) (où `pr`$= k[x]$) :
`quoP.<y>=pr.quotient_ring(P)`. Si $f \in k[x]$, alors $f(y)$ est dans $k[x]/(P)$.
Pour relever un élément Q de $k[x]/(P)$ dans $k[x]$: `Q.lift()`.

Listes, boucles

Pour ajouter un élément x à une liste l : `l.append(x)`, ou bien `l=l+[x]`.
Pour la taille d'une liste l : `len(l)`.
Boucle for, pour aller de m à $n-1$: `for i in range(m,n):`

Vecteurs et matrices

Soit V une matrice. Pour modifier le coefficient (i, j) de V en lui affectant une valeur x, taper `V[i,j]=x`.
Pour transformer une liste l en un vecteur v : `v=vector(l)`.
Pour définir un vecteur $v = (1, 2, 3)$: `v=vector([1,2,3])`.
Pour la taille d'un vecteur v : `len(v)`.

Algorithme de Cantor-Zassenhaus en caractéristique impaire.

Algorithme 1. Factorisation dans $\mathbb{F}_q[x]$.

Entrées: $q = p^k$, où p est un nombre premier impair, $Q \in \mathbb{F}_q[x]$ de degré n, produit de polynômes irréductibles deux à deux distincts de degré d.
Sorties: Un diviseur non trivial de Q, ou bien "échec".

1: Tirer au hasard $A \in \mathbb{F}_q[x]$ de degré strictement inférieur à n.
2: Calculer $D = \mathrm{pgcd}(A, Q)$. Si $D \neq 1$, sortir D.
3: Calculer $B = A^{(q^d-1)/2} - 1 \bmod Q$.
4: Calculer $D = \mathrm{pgcd}(B, Q)$. Si $D \neq 1$ et $D \neq Q$, sortir D. Sinon, sortir "échec".
