Université Claude Bernard LYON 1
Master MA Mathématiques générales
Algèbre et calcul formel

Corrigé de la fiche de TD 5

Exercice 1.
Evaluer la complexité du critère d'irréductibilité d'un polynôme sans facteur multiple $F \in \mathbb{F}_p[X]$, puis celle de l'algorithme de Berlekamp.

Corrigé.
Rappelons les complexités suivantes :

1. pour la division euclidienne d'un polynôme de degré m par un polynôme de degré n : $O(n(m-n-+1))$
2. pour le pgcd de deux polynômes de degrés m et n par l'algorithme d'Euclide : $O(mn)$
3. pour le calcul d'une base du noyau d'une matrice d'ordre n : $O(n^3)$

La phase préliminaire de l'algorithme de Berlekamp, qui permet aussi de tester l'irréductibilité ou de déterminer le nombre r de facteurs irréductibles de F se décompose alors des les étapes suivantes :

1. calcul de la matrice de Berlekamp : on effectue n divisions euclidiennes d'un polynôme de degré au plus $p(n-1)$ par un polynôme de degré p : $nO(n((n-1)p+p-1) = O(n^3p)$
2. calcul d'une base du noyau :$O(n^3)$

on obtient donc une complexité de $O(pn^3)$.
Pour trouver une facteur irréductible on calcule p pgcd de F avec un polynôme de degré $\leq n-1$: $O(pn^2)$ donc la complexité est encore de l'ordre $O(pn^3)$.
Enfin pour l'algorithme de factorisation complète on répète au plus $r-1$ fois l'étape précédente d'où une complexité d'ordre $O(pn^3 + (r-1)pn^2)$ et comme on a $r \leq n$ la complexité est encore de l'ordre $O(pn^3)$.

Exercice 2.
Soient $f \in \mathbb{Z}[X]$ et $n = \deg(f)$, montrer que l'on a

$$|\mathrm{discrim}_X(f)| \leq n^n (n+1)^{2n-2} ||f||_\infty^{2n-2}$$

(*indication :* on pourra montrer que $|\mathrm{discrim}_X(f)| \leq n^n M(f)^{2n-2}$ en appliquant le lemme de Hadamard au déterminant de Van der Monde)

Corrigé.
Soient $f = a_n X^n + \cdots + a_1 X + a_0$ de degré n et $z_1, \cdots, z_n \in \mathbb{C}$ les racines de f ; considérons le déterminant de Van der Monde

$$V = \prod_{i<j} (z_i - z_j) = \det \begin{pmatrix} 1 & \cdots & 1 \\ z_1 & \cdots & z_n \\ \vdots & & \vdots \\ z_1^{n-1} & \cdots & z_n^{n-1} \end{pmatrix}$$

Le *discriminant* de f est donné par :

$$\Delta = a_n^{2n-2} V^2$$

Par le *lemme de Hadamard* on obtient :

$$|\Delta| = |a_n|^{2n-2}\,|V|^2 \leq a_n^{2n-2}\prod_{k=1}^{n}(1+|z_k|^2+\cdots+|z_k|^{2n-2})$$

On a pour $1 \leq k \leq n$:

$$|z_k| \leq \max(1,|z_k|)$$

donc

$$s_k = 1+|z_k|^2+\cdots+|z_k|^{2n-2} \leq 1+\max(1,|z_k|)^2+\cdots+\max(1,|z_k|)^{2n-2}$$

mais

$$\max(1,|z_k|) \geq 1$$

donc on a pour

$$0 \leq j \leq n-1$$

$$\max(1,|z_k|)^{2j} \leq \max(1,|z_k|)^{2n-2}$$

de sorte que

$$s_k \leq n\max(1,|z_k|)^{2n-2}$$

et donc

$$\begin{aligned}
|\Delta| &\leq |a_n|^{2n-2}\prod_{k=1}^{n}s_k \\
&\leq |a_n|^{2n-2}n^n\prod_{k=1}^{n}\max(1,|z_k|)^{2n-2} \\
&\leq n^n\,M(f)^{2n-2}
\end{aligned}$$

En appliquant l'inégalité de Landau on a finalement :

$$|\mathrm{discrim}_X(f)| \leq n^n M(f)^{2n-2} \leq n^n||f||_2^{2n-2} \leq n^n(n+1)^{2n-2}||f||_\infty^{2n-2}$$

Exercice 3.

1. Soit K un corps commutatif ; on désignera par $K[X]_{\leq n}$ l'espace vectoriel formé du polynôme nul et des polynômes de degré $\leq n$.
   Soit $x = (x_1, \cdots, x_{n+1})$ une suite de $n+1$ éléments de K *deux à deux distincts* ; alors montrer que l'application linéaire :
   $$\begin{array}{rcl} L_x : K[X]_{\leq n} & \longrightarrow & K^{n+1} \\ f & \longrightarrow & (f(x_1), \cdots, f(x_{n+1})) \end{array}$$
   est bijective.
   Pour $1 \leq i \leq n+1$, considérons le polynôme :
   $$L_{x,i} = \frac{\prod\limits_{k \neq i}(X - x_k)}{\prod\limits_{k \neq i}(x_i - x_k)}$$
   Pour tout $y = (y_1, \cdots, y_{n+1}) \in K^{n+1}$, on pose $f = \sum\limits_{i=1}^{n+1} y_i L_{x,i} \in K[X]_{\leq n}$; montrer que $L_x(f) = y$ (polynômes d'interpolation de Lagrange).
2. Soit $f \in \mathbb{Z}[X]$ un polynôme primitif de degré n avec $n = 2s$ ou $n = 2s+1$.
   On fixe une suite strictement croissante d'entiers $(x_1, \cdots, x_{s+1})$ dont aucune n'est racine de f.
   Soit $g \in \mathbb{Z}[X]$ un diviseur de f de degré $\leq s$; montrer que g est déterminé de manière unique par les entiers $y_i = g(x_i)$ pour $1 \leq i \leq s+1$ et que l'on a $y_i | f(x_i)$ pour $1 \leq i \leq s+1$.
   En déduire un algorithme permettant de factoriser f (algorithme de Kronecker).

Corrigé.

1. Soit $x = (x_1, \cdots, x_{n+1})$ une suite de $n+1$ éléments de K *deux à deux distincts* ; alors l'application linéaire :
$$\begin{array}{rcl} L_x : K[X]_{\leq n} & \longrightarrow & K^{n+1} \\ f & \longrightarrow & (f(x_1), \cdots, f(x_{n+1})) \end{array}$$
est bijective : L_x est injective car si un polynôme f *non nul* de degré $\leq n$ vérifiait $f(x_i) = 0$ pour $1 \leq i \leq n+1$ il possèderait au moins $n+1$ racines ; par égalité des dimensions l'application L_x est surjective.
Pour $1 \leq i \leq n+1$, on pose :
$$L_{x,i} = \frac{\prod\limits_{k \neq i}(X - x_k)}{\prod\limits_{k \neq i}(x_i - x_k)}$$
de sorte que
$$L_{x,i}(x_k) = \delta_{i,k}$$
Les $n+1$ formes linéaires
$$\epsilon_{x_i} : f \longrightarrow f(x_i)$$
sur $K[X]_{\leq n}$ sont *linéairement indépendantes* : si l'on a une combinaison linéaire $\sum\limits_{k=1}^{n+1} \lambda_k f(x_k) = 0$ pour tout $f \in K[X]_{\leq n}$ en prenant $f = L_{x,i}$ on a $\lambda_i = 0$. Il en résulte que ces formes constituent une base de $K[X]_{\leq n}$. Ainsi $(L_{x,i})_{1 \leq i \leq n+1}$ est la *base duale* de la base $(\epsilon_{x,i})_{1 \leq i \leq n+1}$ de sorte que tout $f \in K[X]_{\leq n}$ s'écrit de manière *unique* $f = \sum\limits_{i=1}^{n+1} f(x_i) L_{x,i}$.

2. Il s'agit de montrer qu'il existe un algorithme permettant de factoriser un polynôme primitif $f \in \mathbb{Z}[X]$ de degré $n = 2s$ ou $n = 2s + 1$. Remarquons tout d'abord qu'il suffit de rechercher les facteurs $g \in \mathbb{Z}[X]$ tels que $\deg(g) \leq s$.
Pour cela on part d'une liste $x = [x_1, \cdots, x_{s+1}]$ de $s + 1$ entiers deux à deux distincts dont aucun n'est racine de f. Ensuite on remarque que si $g \in \mathbb{Z}[X]$ est un facteur de f de degré $\leq s$, $y_i = g(x_i)$ est un diviseur $f(x_i)$ pour $1 \leq i \leq s$.
La méthode de Kronecker consiste à former toutes les suites d'entiers $y = (y_1, \cdots, y_{s+1})$ telles que $y_i | f(x_i)$ pour $1 \leq i \leq s+1$ et à calculer le polynôme d'interpolation de Lagrange g correspondant. Si g est à coefficient entiers, divise f et que le quotient $h = \dfrac{f}{g}$ est lui aussi à coefficients entiers ,alors g (*resp.* h) est un facteur de f de degré $\leq s$ (*resp.* $\geq s$).
Remarquons que l'ensemble des suites d'entiers $y = (y_1, \cdots, y_{s+1})$ telles que $y_i | f(x_i)$ pour $1 \leq i \leq s + 1$ est fini, parce qu'un entier *positif* n'a qu'un nombre fini de diviseurs *positifs* et que l'anneau $\mathbb{Z}$ ne contient qu'un nombre fini d'éléments *inversibles*.

Algorithme 1 *Factorisation de Kronecker*

1. *entrée : un polynôme primitif* $f \in \mathbb{Z}[X]$
2. *initialisations :* $n := \deg(f)$ $s := [n/2]$ $F := \emptyset$
3. *déterminer une liste* $x = [x_1, \cdots, x_{s+1}]$ *d'entiers deux à deux distincts qui ne sont pas racines de* f.
4. *calculer* $\mathcal{D}_i$ *l'ensemble des diviseurs (positifs et négatifs) de* $f(x_i)$ *pour tout* i, $1 \leq i \leq s+1$,.
5. *pour tout* $y = (y_1, \cdots, y_{s+1}) \in \mathcal{D}_1 \times \cdots \times \mathcal{D}_{s+1}$ *déterminer le polynôme de Lagrange* $g \in \mathbb{Q}[X]$ *tel que* $g(x_i) = y_i$ *pour* $1 \leq i \leq s + 1$.
   Si $g \in \mathbb{Z}[X]$, *divise* f *et si* $h = \dfrac{f}{g} \in \mathbb{Z}[X]$ *alors rajouter* g *et* h *à l'ensemble* F.
6. *sortie : l'ensemble des diviseurs de* f