ÉNS de Lyon
2018-2019

Agrégation
Option C

TD Polynômes 2

Exercice 1 — Suites de Sturm — En utilisant les suites de Sturm, déterminer le nombre de racines réelles des polynômes suivants :

1. $P(x) = x^2 + bx + c$ avec $b, c \in \mathbb{R}$ quelconques ;
2. $P(x) = x^4 - x^3 - x - 1$.

Exercice 2 — Algorithme de Berlekamp — Soit p un nombre premier. L'algorithme de Berlekamp permet de déterminer, à l'aide d'outils d'algèbre linéaire, tous les facteurs irréductibles d'un polynôme sans facteur carré de $\mathbb{F}_p[X]$.

1. Soit $P \in \mathbb{F}_p[X]$ un polynôme quelconque, et A l'anneau quotient $\mathbb{F}_p[X]/(P)$. Montrer que l'application $\varphi : A \to A$ définie par $\varphi(a) = a^p$ est un morphisme d'anneaux et est $\mathbb{F}_p$-linéaire.

Soit maintenant $P \in \mathbb{F}_p[X]$ un polynôme unitaire sans facteur carré. Notons $P = P_1 \cdots P_r$ où les P_i sont unitaires irréductibles et premiers entre eux dans $\mathbb{F}_p[X]$. Posons $A = \mathbb{F}_p[X]/(P)$ et $K_i = \mathbb{F}_p[X]/(P_i)$.

2. Expliciter un isomorphisme de $\mathbb{F}_p$-algèbres $A \cong K_1 \times \cdots \times K_r$.
3. Démontrer que l'on a $r = \dim_{\mathbb{F}_p} \ker(\varphi - \mathrm{Id}_A)$. En déduire un critère d'irréductibiité pour P.

Supposons désormais que P est réductible dans $\mathbb{F}_p[X]$.

4. Justifier l'existence d'un polynôme $Q \in \mathbb{F}_p[X]$ non congru à un polynôme constant modulo P et tel que $\overline{Q} \in \ker(\varphi - \mathrm{Id}_A)$.
5. Montrer que $P = \displaystyle\prod_{\alpha \in \mathbb{F}_p} \mathrm{pgcd}(P, Q - \alpha)$.
6. Montrer qu'il existe $\alpha \in \mathbb{F}_p$ tel que $\mathrm{pgcd}(P, Q - \alpha)$ est un facteur non trivial de P.
7. En déduire un algorithme permettant de trouver les facteurs irréductibles de P.
8. Quel est le coût de cet algorithme ?
9. Comment généraliser cet algorithme pour factoriser dans $\mathbb{F}_q[X]$, où $\mathbb{F}_q$ est un corps fini ?

Exercice 3 — Application à la factorisation dans $\mathbb{Z}[X]$ — Considérons l'algorithme suivant : soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de discriminant $\Delta(P)$ non nul.

- On détermine un entier $M \geq 2^{\deg P} \|P\|_2$.
- On choisit un nombre premier p ne divisant pas $\Delta(P)$ tel que $p \geq 2M + 1$.
- Par l'algorithme de Berlekamp, on détermine les facteurs irréductibles unitaires $P_1, \ldots, P_r \in \mathbb{F}_p[X]$ de la réduction de P modulo p.

— Pour toute partie non vide et stricte I de $\{1,\ldots,r\}$, on calcule le polynôme $P_I := \prod_{i\in I} P_i$ et l'on choisit un représentant unitaire $Q_I \in \mathbb{Z}[X]$ de P_I vérifiant $\|Q_I\|_\infty \leq \frac{p}{2}$.

— On teste si Q_I divise P dans $\mathbb{Z}[X]$.

- Si oui, alors Q_I est un facteur non trivial de P dans $\mathbb{Z}[X]$; de plus, si aucun Q_J avec J strictement inclus dans I ne divise P, alors Q_I est un facteur irréductible de P et l'on peut se limiter à étudier les polynômes Q_J avec J inclus dans le complémentaire de I pour obtenir les autres facteurs irréductibles de P.
- Si aucun Q_I ne divise P, alors P est un polynôme irréductible.

1. Pourquoi fait-on l'hypothèse $\Delta(P) \neq 0$?
2. Expliquer pourquoi dans ce cas, l'algorithme présenté fonctionne et permet effectivement d'obtenir tous les facteurs irréductibles de P dans $\mathbb{Z}[X]$.
3. Estimer le coût de cet algorithme.

On peut améliorer cet algorithme en travaillant modulo p^N, où p et N sont choisis de telle sorte que $p^N \geq 2M+1$, et en utilisant le lemme de Hensel pour déterminer une factorisation dans $\mathbb{Z}/p^N\mathbb{Z}[X]$ à partir d'une factorisation dans $\mathbb{F}_p[X]$.