ÉNS de Lyon — Option C
M2 FEADéP — 2020–2021

TD Polynômes

Exercice 1 — Calculs dans $\mathbb{Z}[X]$ —

Estimer le coût du calcul de la somme et du produit de deux polynômes $P, Q \in \mathbb{Z}[X]$ en fonction de leurs degrés et d'une borne uniforme M de la valeur absolue de leurs coefficients.

Exercice 2 — Borne de Mignotte et application à la factorisation dans $\mathbb{Z}[X]$ —

À tout polynôme $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$, on associe les quantités suivantes :

$$\|P\|_\infty := \max_{0\le k\le n} |a_k| \ ; \ \|P\|_2 := \sqrt{\sum_{k=0}^{n} |a_k|^2} \ ; \ \|P\|_1 := \sum_{k=0}^{n} |a_k| \ .$$

En outre, si l'on a $P(X) = a_n \prod_{k=1}^{n} (X - z_k)$, on définit $M(P) := |a_n| \prod_{k=1}^{n} \max(1, |z_k|)$.

1. Vérifier que pour tous polynômes $P, Q \in \mathbb{C}[X]$, on a $M(PQ) = M(P)M(Q)$.

2. Montrer que pour tout polynôme $P \in \mathbb{C}[X]$ et tout élément $z \in \mathbb{C}$, on a

$$\|(X - z)P(X)\|_2 = \|(\bar{z}X - 1)P(X)\|_2 \ .$$

3. Démontrer que pour tout $P \in \mathbb{C}[X]$, on a $M(P) \le \|P\|_2$.

4. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$. Montrer que l'on a $|a_k| \le \binom{n}{k} M(P)$.

On suppose maintenant $P \in \mathbb{Z}[X]$. Soit $Q = \sum_{k=0}^{m} b_k X^k \in \mathbb{Z}[X]$ un polynôme divisant P dans $\mathbb{Z}[X]$.

5. Montrer que pour tout $0 \le k \le m$, on a $|b_k| \le \binom{m}{k} \|P\|_2$.

6. En déduire une méthode pour factoriser les polynômes de $\mathbb{Z}[X]$.

Exercice 3 — Algorithme de Berlekamp —

Soit p un nombre premier. L'algorithme de Berlekamp permet de factoriser les polynômes sans facteur carré de $\mathbb{F}_p[X]$ grâce à des outils d'algèbre linéaire.

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. Montrer que $r = \dim_{\mathbb{F}_p} \ker(\varphi - \mathrm{Id}_A)$. En déduire un critère d'irréductibilité pour P.

On suppose 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 $P = \prod_{\alpha \in \mathbb{F}_p} \mathrm{pgcd}(P, Q - \alpha)$.

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 4 — 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 $\mathbb{F}_p[X]$.

Exercice 5 — Construction de corps finis —

On rappelle que pour construire un corps fini K à $q = p^n$ éléments, avec p premier, il suffit de trouver un polynôme irréductible $P \in \mathbb{F}_p[X]$ de degré n, et poser $K = \mathbb{F}_p[X]/(P)$. On note $a(n)$ le nombre de polynômes unitaires irréductibles de degré n dans $\mathbb{F}_p[X]$.

1. Montrer que $p^n = \sum_{d|n} a(d)$.

2. Montrer que $a(n) = \frac{1}{n}\sum_{d|n} p^d \mu(\frac{n}{d})$, où μ est la fonction de Möbius définie par

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^r & \text{si } n = p_1 \cdots p_r \text{ avec } p_i \text{ premiers distincts}, \\ 0 & \text{si } n \text{ est divisible par } p^2 \text{ avec } p \text{ premier}. \end{cases}$$

3. Montrer que $a(n) \geq \frac{1}{n}\big(p^n - \frac{p^n - p}{p-1}\big)$.

4. On considère l'algorithme probabiliste suivant :

Choisir au hasard $P \in \mathbb{F}_p[X]$ de degré n ;
Tester si P est irréductible (par exemple avec l'algorithme de Berlekamp) ;
Si P est irréductible, renvoyer P, sinon recommencer.

Estimer le nombre moyen d'étapes nécessaires pour obtenir un polynôme irréductible.

Exercice 6 — Méthode de Karatsuba pour les entiers —

Soit $n = 2m$ un entier pair, et soient a, b des entiers s'écrivant avec au plus n bits.

1. Vérifier que l'algorithme suivant calcule le produit ab :

Ecrire $a = \alpha_1 2^m + \alpha_0$ avec $0 \leq \alpha_0, \alpha_1 < 2^m$;
Ecrire $b = \beta_1 2^m + \beta_0$ avec $0 \leq \beta_0, \beta_1 < 2^m$;
Poser $x \leftarrow (\alpha_0 + \alpha_1)(\beta_0 + \beta_1)$;
Poser $y \leftarrow \alpha_1\beta_1$;
Poser $z \leftarrow \alpha_0\beta_0$;
Renvoyer $y2^n + (x - y - z)2^m + z$.

2. Pourquoi cet algorithme est-il plus rapide que l'algorithme classique ?

Exercice 7 — Méthode de Karatsuba pour les polynômes —

Soit K un corps. Soient $P, Q \in K[X]$ des polynômes de degré $\leq 2n$. On écrit

$$P(X) = P_0(X) + P_1(X)X^n, \qquad Q(X) = Q_0(X) + Q_1(X)X^n$$

où P_0, P_1, Q_0, Q_1 sont des polynômes de degré $\leq n$.

1. Montrer que l'on a $PQ = P_1Q_1 \cdot X^{2n} + \big[(P_0+P_1)(Q_0+Q_1) - P_0Q_0 - P_1Q_1\big] \cdot X^n + P_0Q_0$.

On note $T(n)$ le nombre de multiplications dans K nécessaires pour calculer le produit de deux polynômes de degré $\leq n$ avec la méthode ci-dessus (on néglige le coût des additions).

2. Montrer $T(2n) = 3T(n)$ et en déduire $T(n) = O(n^{\log_2(3)})$.

3. Comparer avec l'algorithme classique.