Rappels et anneaux de polynômes

Exercice 1. (Exponentiation rapide).
Écrire une procédure calculant une puissance par exponentiation rapide. Estimer la complexité.

Exercice 2. (Méthode de Horner).
Écrire une fonction d'évaluation à l'aide de la méthode de Horner. Écrire une fonction implémentant l'évaluation naive. Illustrer les résultats du cours.

Exercice 3. (Décomposition sans carré.)
Soit K de caractéristique nulle ou $K = \mathbb{Z}/p\mathbb{Z}$. Pour un polynôme $P \in \mathbb{K}[X]$ unitaire, on note $P = P_1^{r_1} \cdots P_k^{r_k}$ sa décomposition en facteurs irréductibles. La *partie sans carré* de P est $P_1 \cdots P_k$. On dit que P est *sans carré* s'il est égal à sa partie sans carré. Montrer que le polynôme $P \in K[X]$ est sans carré si et seulement si P et P' sont premiers entre eux.

Exercice 4. (Décomposition sans carré dans $\mathbb{Q}$).

(1) Expliquer comment trouver la partie sans carré d'un polynôme (unitaire) dans $\mathbb{Q}[X]$ sans le factoriser.

(2) Écrire une procédure calculant la partie sans carré d'un polynôme $P \in \mathbb{Q}[X]$ sans le factoriser.

(3) Montrer que tout polynôme $P \in \mathbb{Q}[X]$ unitaire de degré n peut s'écrire $P = Q_1(Q_2)^2 \cdots (Q_n)^n$ où les $Q_i \in \mathbb{Q}[X]$ sont sans carré et premiers entre eux. On parle de *décomposition sans carré*.

(4) Expliquer comment calculer la décomposition sans carré d'un polynôme (unitaire) sans le factoriser.

(5) Écrire une procédure calculant la décomposition sans carré d'un polynôme $P \in \mathbb{Q}[X]$ sans le factoriser.

Exercice 5. (Partie sans carré dans $\mathbb{Z}/p\mathbb{Z}$).

(1) Soit $P = P_1^{m_1} \cdots P_r^{m_r} \in \mathbb{F}_p[X]$ unitaire où les P_i sont deux à deux distincts. Montrer que $P/\mathrm{pgcd}(P, P') = \prod_{p \wedge m_i = 1} P_i$.

(2) Expliquer comment calculer $R = \prod_{p \wedge m_i \neq 1} P_i^{m_i}$ sans factoriser P.

(3) Expliquer comment calculer la partie sans carré de $P \in \mathbb{Z}/p\mathbb{Z}[X]$ (unitaire) sans factoriser P.

(4) Écrire une procédure calculant la partie dans carré dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 6. Soit $K = \mathbb{Z}/2\mathbb{Z}(Y)$ et $P(X) = X^2 + Y \in K[X]$.

(1) Montrer que P est irréductible.

(2) Vérifier votre résultat avec `sage`.

(3) Les polynômes P et P' sont-ils premiers entre eux ?

Exercice 7. (Dichotomie).
Écrire une procédure basée sur la dichotomie prenant en entrée un polynôme $P \in \mathbb{Q}[X]$, $a < b$ tels que $P(a)P(b) < 0$ et $\epsilon > 0$ et renvoyant une valeur approchée à ϵ-près d'une racine de P dans $[a, b]$.

Exercice 8. (Méthode de Newton).

(1) Écrire la méthode de Newton sous la forme d'une fonction prenant en entrée une fonction (dont on cherche un zéro), sa dérivée, le point de départ de l'itération de Newton et le nombre d'itérations à effectuer.

(2) Tester votre fonction avec $f : x \mapsto x^3 - 2$. Illustrer la convergence quadratique.

(3) Comparer avec la dichotomie.

(4) Tester votre fonction avec $f : x \mapsto x^3 - 2x^2 + 11x + 12$ et pour points de départ 2.3528, 2.35286 et 2.35288.

(5) Tester votre fonction avec $f : x \mapsto x^3 - 2x + 2$ avec pour point de départ 0.

Exercice 9. (Lemme de Hensel).

(1) Soit $P \in \mathbb{Z}[X]$, p premier et $n \geqslant 1$. On suppose qu'il existe $x \in \mathbb{Z}$ tel que $P(x) \equiv 0[p^n]$ et $P'(x) \not\equiv 0[p]$. Montrer qu'il existe un unique $\overline{y} \in \mathbb{Z}/p^{2n}\mathbb{Z}$ tel que $P(y) \equiv 0[p^{2n}]$ et $x \equiv y[p^n]$ où y est un relevé de $\overline{y}$. *On pourra écrire* $P(X + H) = P(X) + HP'(X) + H^2R(X)$.

(2) Écrire une procédure `hensel` prenant en entrée un polynôme $P \in \mathbb{Z}[x]$, un nombre premier p, un entier x vérifiant $P(x) \equiv 0 \,(\mathrm{mod}\, p)$ et $P'(x) \not\equiv 0 \,(\mathrm{mod}\, p)$, et un entier $m \geqslant 1$, et renvoyant un entier y tel que $x \equiv y \,(\mathrm{mod}\, p)$ et $P(y) \equiv 0 \,(\mathrm{mod}\, p^{2^m})$.

(3) En utilisant cette fonction, déterminer les racines carrées de 2 dans $\mathbb{Z}/7^{32}\mathbb{Z}$.

Exercice 10. Soit $P = x^3 + 2x + 16$.

(1) Avec `sage`, factoriser $\bar{P}$, la réduction de P modulo 11 .

(2) En utilisant la fonction `hensel`, déterminer l'unique racine de P modulo 11^2 (pourquoi cette racine est-elle unique ?).

(3) En utilisant des bornes sur les racines, déduire que P est irréductible dans $\mathbb{Z}[x]$.

Exercice 11. Soit $P = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}[x]$.

(1) Factoriser P modulo 2 et modulo 13.

(2) Déduire que P est irréductible dans $\mathbb{Z}[x]$.

Exercice 12 (Méthode de Graeffe (1826))**.** Soit $P \in \mathbb{C}[X]$ unitaire de degré n. On note $z_1, \ldots, z_n$ ses racines (avec répétition s'il y a des racines multiples).

(1) Expliquer comment obtenir, sans déterminer les racines de P, un polynôme Q unitaire de degré n dont les racines sont exactement $z_1^2, \ldots, z_n^2$.
On pourra considérer $P(X)P(-X)$.

(2) On suppose maintenant que z_n est réelle et strictement plus grande que 1 et que toutes les autres racines de P sont de module strictement plus petit que 1. On considère la suite de polynômes (P_m) définie par $P_0 = P$ et P_j est obtenu à partir de P_{j-1} en appliquant le procédé décrit dans la question précédente. Soit $\rho < 1$ un majorant du module des racines différentes de z_n. Estimer les coefficients de degré $n - 1$ de la suite (P_m) à l'aide de z_n, m et ρ.

(3) Illustrer avec `sage`.