TD – Lemme de Hensel et factorisation des polynômes

Lemme de Hensel

Exercice 1. (Lemme de Hensel simplifié) Soient p un nombre premier, $P \in \mathbb{Z}[X]$ et $n \geqslant 1$ un entier. On suppose qu'il existe $a \in \mathbb{Z}$ tel que $P(a) \equiv 0 \bmod p^n$ et $P'(a) \not\equiv 0 \bmod p$.

Montrer qu'il existe un entier b tel que $a \equiv b \bmod p^n$ et $P(b) \equiv 0 \bmod p^{2n}$, et que $b \bmod p^{2n}$ est uniquement déterminé.

Exercice 2. (Lemme de Hensel) Soient p un nombre premier, $P \in \mathbb{Z}[X]$ et $n \geqslant 1$ un entier. Soit a un entier tel que $P'(a)$ soit non nul. On note v la valuation p-adique de $P'(a)$. Supposons que $n \geqslant 2v+1$.

1. Montrer que si b est un entier égal à a modulo p^{n-v}, alors $P(a) \equiv P(b) \bmod p^n$, et la valuation p-adique de $P'(b)$ est v.
2. On suppose de plus que $P(a) \equiv 0$ modulo p^n. Montrer qu'il existe $b \in \mathbb{Z}$ tel que $a \equiv b \bmod p^{n-v}$ et $P(b) \equiv 0 \bmod p^{2(n-v)}$, et que $b \bmod p^{2n-3v}$ est entièrement déterminé.

Exercice 3.

1. Soit p premier impair. Montrer que $a \in \mathbb{Z}$ est un carré modulo p si et seulement si a est un carré modulo p^n pour tout n.
2. Montrer qu'un entier impair a est un carré modulo 2^n pour tout n si et seulement si $a \equiv 1 \bmod 8$.

Exercice 4. (Contre-exemple au principe de Hasse) Montrer que l'équation suivante :

$$(x^2-2)(x^2-17)(x^2-34) = 0$$

a des solutions modulo tout entier non nul, mais n'a pas de solution rationnelle.

Factorisation de polynômes

Exercice 5. (Algorithme de Berlekamp) Soit $P \in \mathbb{Z}/p\mathbb{Z}[X]$ un polynôme dont on cherche la décomposition en facteurs irréductibles. On pose $A = \mathbb{Z}/p\mathbb{Z}[X]/(P)$.

1. Expliquer comment, si on sait factoriser les polynômes sans facteur carré, on peut factoriser tous les polynômes (de $\mathbb{Z}/p\mathbb{Z}[X]$).

   On suppose P désormais unitaire et sans facteur carré.
2. Montrer que si $Q \in \mathbb{Z}/p\mathbb{Z}[X]$ vérifie la relation $Q^p \equiv Q \bmod P$, alors $P = \prod_{a \in \mathbb{Z}/p\mathbb{Z}} \operatorname{pgcd}(P, Q-a)$.
3. Soit $P = P_1 \cdots P_r$ la décomposition de P en facteurs irréductibles. Montrer que $Q^p \equiv Q \bmod P$ si, et seulement s'il existe $(a_1, \ldots, a_k) \in (\mathbb{Z}/p\mathbb{Z})^k$ tel que $Q \equiv a_i \bmod P_i$ pour tout $i \in [\![1, k]\!]$, et qu'à chaque $(a_1, \ldots, a_k) \in (\mathbb{Z}/p\mathbb{Z})^k$ correspond un unique polynôme $Q \bmod P$ vérifiant cette propriété.
4. En déduire que l'algorithme suivant, dû à Berlekamp, se termine et fournit bien la décomposition en facteurs irréductibles d'un polynôme de $\mathbb{Z}/p\mathbb{Z}[X]$ sans facteur carré :
   (a) Soit $S : A \to A$ le morphisme défini par $S(X) = X^p$; on calcule la matrice de l'endomorphisme $S - \mathrm{Id}$ dans la base canonique $(1, \bar{X}, \ldots, \bar{X}^{\deg(P)-1})$ de A.
   (b) Si $\dim(\ker(S - \mathrm{Id}))$ est égal à 1, alors P est irréductible et on arrête l'algorithme. Sinon, on passe à l'étape suivante.

(c) On calcule un polynôme Q dont l'image dans A est non constante, et dans $\ker(S - \mathrm{Id})$. Avec l'algorithme d'Euclide, on calcule les $\mathrm{pgcd}(P, Q - a)$ pour a parcourant $\mathbb{Z}/p\mathbb{Z}$. On a alors $P = \prod_{a \in \mathbb{Z}/p\mathbb{Z}} \mathrm{pgcd}(P, Q - a)$, et on retourne à l'étape (a) pour chaque facteur non trivial du produit.

Exercice 6. (Lemme de Hensel pour la factorisation des polynômes) Soient p un nombre premier, et $P \in \mathbb{Z}[X]$ unitaire. Soit $n \geqslant 1$ un entier. On suppose qu'il existe une factorisation $P = QR$ modulo p^n où Q et R sont unitaires et premiers entre eux modulo p. Montrer qu'il existe une factorisation $P = \tilde{Q}\tilde{R}$ modulo p^{2n}, où $\tilde{Q}$ et $\tilde{R}$ sont unitaires et se réduisent respectivement en Q et R modulo p^n.

Exercice 7. (Inégalité de Mignotte) Pour tout polynôme $P = \sum_{i=0}^{m} a_i X^i \in \mathbb{R}[X]$, posons

$$\|P\|_2 = \sqrt{\sum_{i=0}^{m} a_i^2}.$$

Si on note α_i les racines de P (complexes, comptées avec multiplicités), on pose également

$$\hat{P} = a_m \prod_{|\alpha_i| \geqslant 1} (X - \alpha_i) \prod_{|\alpha_i| < 1} (\bar{\alpha_i} X - 1).$$

1. Montrer que $\|\hat{P}\| = \|P\|$.
2. Si $x_1, \ldots, x_m \geqslant 1$, montrer que $\sum_{1 \leqslant i_1 < \cdots < i_k \leqslant m} x_{i_1} \cdots x_{i_k} \leqslant \binom{m-1}{k-1} \prod_{i=1}^{m} x_i + \binom{m-1}{k}$.
3. Montrer que si $P = \sum_{i=0}^{m} a_i X^i \in \mathbb{Z}[X]$ a pour racines α_i (complexes, comptées avec multiplicités), alors $|a_j| \leqslant |a_m| \left(\binom{m-1}{j} \prod_{i=1}^{m} \max(1, |\alpha_i|) + \binom{m-1}{j-1} \right)$.
4. En déduire l'inégalité de Mignotte : soient $P = \sum_{i=0}^{m} a_i X^i \in \mathbb{Z}[X]$ et $Q = \sum_{j=0}^{n} b_j X^j \in \mathbb{Z}[X]$ un diviseur de P. Alors, pour tout $j \in [\![0, n]\!]$, on a $|b_j| \leqslant \binom{n-1}{j} \|P\|_2 + \binom{n-1}{j-1} |a_m|$.

Exercice 8. (Factorisation dans $\mathbb{Z}$) Expliquer comment obtenir une factorisation dans $\mathbb{Z}$ d'un polynôme P à partir de l'algorithme de Berlekamp et du lemme de Hensel (on appliquera l'algorithme et le lemme avec un nombre premier p tel que $\mathrm{pgcd}(P, P') \equiv 1 \bmod p$ et tel que le coefficient dominant de P soit inversible modulo p).