Calcul Formel - Master 1 - Univ. Paris-Saclay

Chapitre 7 - Partie 1

I Lemme de Hensel et relèvement de factorisations.

1) Lemme de Hensel.

Prop : Soit $P \in \mathbb{Z}[X]$ unitaire, et p un nombre premier. Soit $n \in \mathbb{N}^*$ et $x \in \mathbb{Z}$ tel que $P(x) \equiv 0 \ [p^n]$ et $P'(x) \not\equiv 0 \ [p]$. Alors il existe $\tilde{x} \in \mathbb{Z}$, unique modulo p^{2n}, tel que $P(\tilde{x}) \equiv 0 \ [p^{2n}]$ et $\tilde{x} \equiv x \ [p^n]$.

Si on voit $x \in \mathbb{Z}/p^{2n}\mathbb{Z}$ on a $\tilde{x} = x - \dfrac{P(x)}{P'(x)}$ avec $\dfrac{1}{P'(x)} = (P'(x))^{-1} \in \left(\mathbb{Z}/p^{2n}\mathbb{Z}\right)^*$.

Prop : Soit $P \in \mathbb{Z}[X]$ unitaire, p premier, et $x \in \mathbb{Z}$ tel que $p \mid P(x)$ et $p \nmid P'(x)$. Soit $N \geq 1$. On pose $x_{n+1} = x_n - \dfrac{P(x_n)}{P'(x_n)}$ avec $x_n \in \mathbb{Z}/p^N\mathbb{Z}$, $x_0 = x \bmod p^N$.

Alors la suite $(x_n)_{n \geq 0}$ est stationnaire à partir de $n = \lceil \log_2 N \rceil$ et sa valeur x_n vérifie alors $P(x_n) = 0$ dans $\mathbb{Z}/p^N\mathbb{Z}$.

2) Relèvement de factorisations.

Prop : Soit $P \in \mathbb{Z}[X]$ unitaire de degré d, et p premier. Soient $n \in \mathbb{N}^*$ et $Q_0, R_0 \in (\mathbb{Z}/p^n\mathbb{Z})[X]$ unitaires de degrés respectifs q et r tels que $\overline{P} = Q_0 R_0$ (en notant $\overline{P}$ la réduction de P modulo p^n).

On suppose que $\mathrm{Res}(Q_0, R_0) \not\equiv 0 \ [p]$. Alors pour tout $m \geq n$ il existe $Q, R \in (\mathbb{Z}/p^m\mathbb{Z})[X]$ uniques, unitaires, de degrés respectifs q et r, qui se réduisent modulo p^n sur Q_0 et R_0, et tels que $P \equiv QR \mod p^m$.

De plus on peut trouver Q, R effectivement.

Cas particulier : $x \in \mathbb{Z}/p^n\mathbb{Z}$, $Q_0(x) = X - x$, $\overline{P}(X) = (X-x)\,R_0(X)$ dans $(\mathbb{Z}/p^n\mathbb{Z})[X]$

Ici $\mathrm{Res}(Q_0, R_0) = R_0(x) = P'(x) \mod p^n$.

Chapitre 7 - Partie 2

II Mesure de Mahler et borne de Mignotte.

1) Mesure de Mahler.

Soit $P \in \mathbb{C}[X]$, $P = \sum_{i=0}^{\deg P} a_i X^i$. On pose : $\|P\|_\infty = \max_i |a_i|$, $\|P\|_1 = \sum_i |a_i|$, $\|P\|_2 = \sqrt{\sum_i |a_i|^2}$

Déf : On pose $M(P) = |a_n| \prod_{k=1}^{n} \max(1, |z_k|)$

avec $n = \deg P$ et $P(X) = a_n \prod_{k=1}^{n} (X - z_k)$.

(avec $M(P) = 0$ si $P = 0$). C'est la mesure de Mahler de P.

Propriété : $M(PQ) = M(P)\,M(Q)$.

Th : Soit $P \in \mathbb{C}[X] \setminus \{0\}$ de degré d. Alors on a :

$$\|P\|_\infty \leq \|P\|_1 \leq 2^{\deg P} M(P) \leq 2^{\deg P} \|P\|_2 \leq 2^{\deg P} \sqrt{\deg P + 1}\, \|P\|_\infty .$$

triviale — cf. Poly — Th. Landau — $\|P\|_2^2 = \sum |a_i|^2 \leq (\deg P + 1) \|P\|_\infty^2$

2) Borne de Mignotte.

Th : Soient $P, Q \in \mathbb{C}[X]$ tel que Q divise P. Notons a_n le coefficient dominant de P et b_m celui de Q. Alors on a :
$$\|Q\|_\infty \leq \frac{|b_m|}{|a_n|} 2^{\deg Q} \|P\|_2 .$$

Lemme : Sous les mêmes hypothèses on a :
$$M(Q) \leq \frac{|b_m|}{|a_n|} M(P).$$

Preuve : $P = QR$ avec $M(R) \geq \frac{|a_n|}{|b_m|}$ et $M(P) = M(Q)\,M(R)$.

III Factorisation dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$.

1) Factorisation dans $\mathbb{Z}[X]$ de polynômes séparables unitaires.

Entrée : $P \in \mathbb{Z}[X]$ unitaire, de discriminant $\mathrm{Disc}(P) \neq 0$, $\deg P \geq 1$.

Sortie : Un facteur irréductible de ~~Q~~ P dans $\mathbb{Z}[X]$ (non constant).

Algorithme : Choisir p premier, $p \nmid \mathrm{Disc}(P)$. Choisir $M \in \mathbb{N}^*$ tel que $M \geq 2^{\deg P} \|P\|_2$.

Choisir $d \in \mathbb{N}^*$ tel que $p^d \geq 2M+1$.

Factoriser P dans $\mathbb{F}_p[X]$: $\overline{P}(X) = Q_1(X) \dots Q_\ell(X)$ — Q_i 2 à 2 $\neq$, Q_i unitaires irréd. $\in \mathbb{F}_p[X]$

Relever cette factorisation dans $\mathbb{Z}/p^d\mathbb{Z}[X]$: $\underbrace{\widetilde{P}}_{\text{réduction de } P \text{ modulo } p^d}(X) = \widetilde{Q}_1(X) \dots \widetilde{Q}_\ell(X)$ dans $(\mathbb{Z}/p^d\mathbb{Z})[X]$ — $\widetilde{Q}_i \in \mathbb{Z}/p^d\mathbb{Z}[X]$ relève Q_i

Pour chaque $I \subsetneq [\![1,\ell]\!]$, $I \neq \emptyset$, on calcule

$\widetilde{Q}_I = \prod_{i \in I} \widetilde{Q}_i \in (\mathbb{Z}/p^d\mathbb{Z})[X]$ et on note $Q_I \in \mathbb{Z}[X]$ tel que Q_I se réduit sur $\widetilde{Q}_I$ mod p^d et $\|Q_I\|_\infty \leq \left\lfloor \frac{p^d}{2} \right\rfloor$

On teste si Q_I divise P. ⚠ on procède par cardinaux de I croissants.

Si oui on renvoie Q_I

Si on ne trouve aucun Q_I qui divise P : on renvoie P.

Correction : Si on note R un facteur irréductible de P, alors $\|R\|_\infty \leq 2^{\deg P} \|P\|_2 \leq M \leq \frac{p^d - 1}{2} \leq \left\lfloor \frac{p^d}{2} \right\rfloor$.

De plus si $\overline{R}$ est sa réduction modulo p alors $\overline{R}(X) = \prod_{i \in I} Q_i(X)$ pour un certain I.

Alors la réduction de R modulo p^d sera $\widetilde{Q}_I$. Alors $R = Q_I$.

2) Extension au cas général.

⊛ Factoriser dans $\mathbb{Z}[X]$ ou dans $\mathbb{Q}[X]$: on passe facilement de l'un à l'autre.
↳ un polynôme de $\mathbb{Z}[X]$ (à condition de savoir factoriser dans $\mathbb{Z}$)

⊛ Dans $\mathbb{Q}[X]$, se ramener à un polynôme séparable : comme $\mathbb{F}_q[X]$.

⊛ Lemme : Soit $P \in \mathbb{Q}[X]$ unitaire. Alors on peut trouver $n \in \mathbb{N}^*$ tel que $n^{\deg P} P(\frac{1}{n}X)$ appartienne à $\mathbb{Z}[X]$ et soit unitaire.

Preuve : notons $P(X) = \sum a_i X^i$ et $d = \deg P$. Alors $n^d P(\frac{1}{n}X) = X^d + n a_{d-1} X^{d-1} + \dots + n^{d-1} a_1 + n^d a_0$.