

Factorisation des polynômes univariés

1 Factorisation dans $\mathbb{F}_p[X]$

On considère un polynôme unitaire $F \in \mathbb{F}_p[X]$, de degré $n \geq 2$ et *sans facteur multiple*¹. L'algèbre $\mathcal{A} = \mathbb{F}_p[X]/\mathbb{F}_p[X]F$ est de rang n sur $\mathbb{F}_p$ de base canonique $(\overline{X^{n-i}})_{1 \leq i \leq n}$: *via* la division euclidienne par F , chaque élément de $\overline{G} \in \mathcal{A}$ est représenté par un *unique* polynôme $G \in \mathbb{F}_p[X]$ avec $G = 0$ ou $\deg(G) \leq n-1$.

On considère l'endomorphisme de Frobenius de $\mathcal{A}$:

$$\begin{aligned} \mathcal{F}_{\mathcal{A}/\mathbb{F}_p} : \mathcal{A} &\longrightarrow \mathcal{A} \\ \overline{G} &\longrightarrow \overline{G^p} \end{aligned}$$

l'algèbre de Berlekamp est la sous-algèbre $\mathcal{A}^{\mathcal{F}_{\mathcal{A}/\mathbb{F}_p}} = \text{Ker}(\mathcal{F}_{\mathcal{A}/\mathbb{F}_p} - \text{Id}_{\mathcal{A}})$ des *points fixes* de $\mathcal{F}_{\mathcal{A}/\mathbb{F}_p}$:

$$\overline{G} \in \mathcal{A}^{\mathcal{F}_{\mathcal{A}/\mathbb{F}_p}} \iff G^p \equiv G \pmod{F}$$

La *matrice de Berlekamp* est la matrice $Q = (Q_{i,j})_{1 \leq i,j \leq n}$ de l'application $\mathbb{F}_p$ -linéaire $\mathcal{Q} = \mathcal{F}_{\mathcal{A}/\mathbb{F}_p} - \text{Id}_{\mathcal{A}}$ dans la base canonique $(\overline{X^{n-i}})_{1 \leq i \leq n}$ de $\mathcal{A}$: pour $1 \leq j \leq n$, $R_j = \sum_{i=1}^n Q_{i,j} X^{n-i}$ est le reste de la division euclidienne de $\mathcal{Q}(X^{n-j}) = X^{p(n-j)} - X^{n-j}$ par F dans $\mathbb{F}_p[X]$.

Proposition 1

Soit $F \in \mathbb{F}_p[X]$ un polynôme unitaire sans facteur multiple ; le rang² r de l'algèbre de Berlekamp $\mathcal{A}^{\mathcal{F}_{\mathcal{A}/\mathbb{F}_p}}$ est égal au nombre r des facteurs irréductibles de F .

On a $r \geq 1$. En particulier F est irréductible si et seulement $\mathcal{A}^{\mathcal{F}_{\mathcal{A}/\mathbb{F}_p}}$ est de rang 1.

∇ Considérons alors la factorisation en polynômes irréductibles $F = F_1 \cdots F_r$. Chacun des polynômes F_i ($1 \leq i \leq r$) étant irréductible, $K_i = \mathbb{F}_p[X]/\langle F_i \rangle$ est une $\mathbb{F}_p$ -extension de degré n_i avec $n_i = \deg(F_i)$. On a $K_i^{\mathcal{F}_{K_i/\mathbb{F}_p}} = \mathbb{F}_p$.

Les polynômes irréductibles F_i , ($1 \leq i \leq r$), étant deux à deux distincts, le *théorème chinois* fournit un isomorphisme de $\mathbb{F}_p$ -algèbres, *compatible* avec les applications de Frobenius :

$$\begin{aligned} \phi : \mathcal{A} &\longrightarrow K_1 \times \cdots \times K_r \\ G \pmod{F} &\longrightarrow (G \pmod{F_1}, \dots, G \pmod{F_r}) \end{aligned}$$

de sorte que ϕ induit un *isomorphisme*³ de $\mathbb{F}_p$ -algèbres :

$$\phi : \mathcal{A}^{\mathcal{F}_{\mathcal{A}/\mathbb{F}_p}} \longrightarrow \mathbb{F}_p^r$$

△

1. ce qui équivaut à $\text{pgcd}(F, F') = 1$ ou à $\text{discrim}_X(F) \neq 0$.
 2. *ie.* la dimension du $\mathbb{F}_p$ -espace vectoriel $\mathcal{A}^{\mathcal{F}_{\mathcal{A}/\mathbb{F}_p}}$, on a $r = n - \text{rg}(Q)$.
 3. Etant donné $G \in \mathbb{F}_p[X]$, on a $\overline{G} \in \mathcal{A}^{\mathcal{F}_{\mathcal{A}/\mathbb{F}_p}}$ si et seulement le reste de la division euclidienne (dans $\mathbb{F}_p[X]$) de G par F_i est une constante $c_i \in \mathbb{F}_p$ pour $1 \leq i \leq r$ et l'on a alors $\phi(\overline{G}) = (c_i)_{1 \leq i \leq r}$.

Proposition 2

Soit $F \in \mathbb{F}_p[X]$ un polynôme unitaire sans facteur multiple ; pour tout $\overline{G} \in \mathcal{A}^{\mathcal{F}_{\mathbb{A}/\mathbb{F}_p}}$ non constant on a la factorisation non triviale de F :

$$F = \prod_{x \in \mathbb{F}_p} \text{pgcd}(F, G - x)$$

∇ On a dans $\mathbb{F}_p[X]$ l'égalité :

$$X^p - X = \prod_{x \in \mathbb{F}_p} (X - x)$$

de sorte que pour tout $G \in \mathbb{F}_p[X]$ avec $\deg(G) \geq 1$ (pour G constant on a une égalité triviale) on a ⁴ :

$$G^p - G = \prod_{x \in \mathbb{F}_p} (G - x)$$

les facteurs $G - x$, $x \in \mathbb{F}_p$, étant deux à deux premiers entre eux ⁵ on a :

$$\text{pgcd}(F, G^p - G) = \prod_{x \in \mathbb{F}_p} \text{pgcd}(F, G - x)$$

Cette factorisation est *non triviale* lorsque $\overline{G}$ n'est pas constant, sinon il existerait $x \in \mathbb{F}_p$ tel que $F = \text{pgcd}(F, G - x)$ de sorte que F diviserait $G - x$. Par division euclidienne ⁶ de G par F on se ramène au cas où $\deg(G) \leq n - 1 < \deg(F)$. Δ

Pour obtenir la factorisation complète de F on applique successivement cette égalité aux éléments G d'une base $(G_k)_{1 \leq k \leq r}$ de $\mathcal{A}^{\mathcal{F}_{\mathbb{A}/\mathbb{F}_p}}$ dans laquelle $G_r = 1$ par l'algorithme suivant :

Algorithme 1 (algorithme de Berlekamp)

1. entrée : $F \in \mathbb{F}_p[X]$ unitaire et sans facteur multiple.
2. initialisation : $\mathcal{E} = \{F\}$ ⁷
3. calculer la matrice de Berlekamp Q
4. calculer une base $G_1, \dots, G_{r-1}, G_r = 1$ de $\mathcal{A}^{\mathcal{F}_{\mathbb{A}/\mathbb{F}_p}}$
5. boucle pour k variant de 1 à $r - 1$:

$\{$
 (a) sortir si $\text{Card}(\mathcal{E}) = r$.
 (b) soit $\mathcal{E} = \{E_1, \dots, E_s\}$; calculer $\tilde{\mathcal{E}}$ l'ensemble des $\text{pgcd}(E_j, G_k - x)$, $1 \leq j \leq s$ et $x \in \mathbb{F}_p$, qui sont non constants ⁸
 (c) $\mathcal{E} := \tilde{\mathcal{E}}$
 $\}$
6. sortie : $\mathcal{E}$ l'ensemble $\{F_1, \dots, F_r\}$ des facteurs irréductibles de F .

4. considérer l'homomorphisme d'algèbre $\phi : \mathbb{F}_p[X] \longrightarrow \mathbb{F}_p[X]$ caractérisé par $\phi(X) = G$

5. si $E_1, \dots, E_s$ sont deux à deux premiers entre eux on a $\text{pgcd}(\prod_{j=1}^s E_j, F) = \prod_{j=1}^s \text{pgcd}(E_j, F)$

6. si R est le reste de la division euclidienne de G par F on a $\text{pgcd}(F, G) = \text{pgcd}(F, R)$

7. En général $\mathcal{E} = \{E_1, \dots, E_s\}$ est un ensemble fini de polynômes unitaires tels que $F = \prod_{j=1}^s E_j$; remarquons que les éléments E_j de $\mathcal{E}$ sont deux à deux premiers entre eux.

8. ie. différents de 1.

▽ Supposons qu'à l'étape $k - 1$ on ait $F = \prod_{j=1}^s E_j$; à l'étape k on a alors :

$$\begin{aligned} F &= \prod_{x \in \mathbb{F}_p} \text{pgcd}(F, G_k - x) \\ &= \prod_{x \in \mathbb{F}_p} \text{pgcd}\left(\prod_{j=1}^s E_j, G_k - x\right) \\ &= \prod_{x \in \mathbb{F}_p} \prod_{j=1}^s \text{pgcd}(E_j, G_k - x) \end{aligned}$$

Si l'on sort de la boucle en (a), le nombre de facteurs non constants de F est égal à r donc ce sont nécessairement les facteurs irréductibles.

Remarquons ensuite qu'un élément $\tilde{E}$ de $\mathcal{E}$ calculé à l'étape k de la boucle est de la forme $\text{pgcd}(E, G_k - s_k)$ où E est un élément de $\mathcal{E}$ obtenu à l'étape $k - 1$; de sorte que $\tilde{E}$ divise $G_k - x_k$ et E donc, en raisonnant par récurrence, divise aussi des éléments $G_j - x_j$ pour $1 \leq j \leq k - 1$. Supposons que l'on a parcouru les $r - 1$ étapes de la boucle et soit $\mathcal{E} = \{E_1, \dots, E_s\}$ l'ensemble obtenu. Ainsi pour tout k , $1 \leq k \leq r - 1$, il existe donc $x_k \in \mathbb{F}_p$ tel que :

$$G_k \equiv x_k \pmod{E}$$

C'est encore vrai pour $k = r$ en prenant $x_r = 1$. Puisque $(G_k)_{1 \leq k \leq r}$ est une base de $A^{\mathcal{F}}$, pour tout $G \in A^{\mathcal{F}/\mathbb{F}_p}$, il existe x_G , $0 \leq s \leq p - 1$ tel que :

$$G \equiv x_G \pmod{E}$$

S'il existait $E \in \mathcal{E}$ qui *ne soit pas irréductible* ; il existerait alors des facteurs irréductibles *distincts* F_i et F_j de F qui diviseraient E . Pour tout $G \in A^{\mathcal{F}}$, on aurait alors :

$$G \equiv x_G \pmod{F_i} \quad G \equiv x_G \pmod{F_j}$$

ce qui contredirait la *surjectivité* de l'homomorphisme :

$$\phi : \mathcal{A}^{\mathcal{F}/\mathbb{F}_p} \longrightarrow \mathbb{F}_p^r$$

Ainsi E_j est irréductible pour $1 \leq i \leq s$ et comme $F = \prod_{j=1}^s E_j$ on a $s = r$ et $E_j = F_j$ pour $1 \leq j \leq r$. Δ

2 Le lemme de Hensel

Proposition 3 (lemme de Hensel)

Soit $F \in \mathbb{Z}[X]$ un polynôme unitaire de degré d ; on suppose donnés des polynômes unitaires $G_1, H_1 \in \mathbb{Z}[X]$, de degrés respectifs r et s , tels que :

1. $\overline{G_1}$ et $\overline{H_1}$ premiers entre eux dans $\mathbb{F}_p[X]$
2. $F \equiv G_1 H_1 \pmod{p\mathbb{Z}[X]}$

Alors pour tout entier $n \geq 2$, il existe des polynômes unitaires $G_n, H_n \in \mathbb{Z}[X]$, uniques modulo $p^n \mathbb{Z}[X]$ vérifiant les conditions suivantes :

1. $G_n \equiv G_{n-1} \pmod{p^{n-1}\mathbb{Z}[X]}$ et $H_n \equiv H_{n-1} \pmod{p^{n-1}\mathbb{Z}[X]}$
2. $F \equiv G_n H_n \pmod{p^n \mathbb{Z}[X]}$

∇ On a $\deg(\overline{G_1}) = r$, $\deg(\overline{H_1}) = s$ et par suite $d = r + s$. De plus, puisque $\overline{G_1}$ et $\overline{H_1}$ sont *premiers entre eux* dans $\mathbb{F}_p[X]$, l'application $\mathbb{F}_p[X]$ -linéaire :

$$\begin{aligned} \partial : K[X]_{\leq s-1} \oplus K[X]_{\leq r-1} &\longrightarrow K[X]_{\leq d-1} \\ (B, A) &\longrightarrow B\overline{G_1} + A\overline{H_1} \end{aligned}$$

est bijective.

On procède *par récurrence* sur $n \geq 2$ en supposant le résultat établi jusqu'à l'ordre $n - 1$.

Puisque

$$\left\{ \begin{array}{l} F \equiv G_{n-1}H_{n-1} \text{ mod } p^{n-1}\mathbb{Z}[X] \\ \deg(G_{n-1}) = r \\ \deg(H_{n-1}) = s \\ F, G_{n-1}, H_{n-1} \text{ sont unitaires} \end{array} \right.$$

il existe un polynôme $C \in \mathbb{Z}[X]$ tel que

$$F = G_{n-1}H_{n-1} + p^{n-1}C \text{ et } \deg(C) \leq d - 1$$

Il existe alors des polynômes $A, B \in \mathbb{Z}[X]$ avec $\deg(A) < r$ et $\deg(B) < s$ tels que⁹ :

$$\overline{G_1} \overline{B} + \overline{H_1} \overline{A} = \overline{C} \text{ dans } \mathbb{F}_p[X]$$

avec $\overline{A}$ et $\overline{B}$ uniques dans $\mathbb{F}_p[X]$.

Notons que :

$$\overline{G_{n-1}} = \overline{G_1} \text{ et } \overline{H_{n-1}} = \overline{H_1}$$

de sorte que :

$$G_{n-1} B + H_{n-1} A = C + p D \text{ avec } D \in \mathbb{Z}[X]$$

On pose alors :

$$G_n = G_{n-1} + p^{n-1}A \text{ et } H_n = H_{n-1} + p^{n-1}B$$

de sorte que G_n et H_n sont *unitaires* et vérifient les conditions :

$$\left\{ \begin{array}{l} \deg(G_n) = \deg(G_{n-1}) \\ \deg(H_n) = \deg(H_{n-1}) \\ G_n \equiv G_{n-1} \text{ mod } p^{n-1} \\ H_n \equiv H_{n-1} \text{ mod } p^{n-1} \end{array} \right.$$

On a de plus :

$$\begin{aligned} F - G_n H_n &= F - (G_{n-1} + p^{n-1}A)(H_{n-1} + p^{n-1}B) \\ &= F - G_{n-1}H_{n-1} - p^{n-1}(G_{n-1}B + H_{n-1}A) - p^{2n-2}AB \\ &= \widehat{p}^{n-1}C - p^{n-1}(C + pD) - p^{2n-2}AB \\ &= p^n D - p^{n-2}AB \end{aligned}$$

d'où finalement :

$$F \equiv G_n H_n \text{ mod } p^n \mathbb{Z}[X]$$

9. L'algorithme d'Euclide étendu permet de calculer des polynômes $U, V \in \mathbb{Z}[X]$ avec $\deg(U) \leq s - 1$ et $\deg(V) \leq r - 1$ tels que :

$$\overline{G_1} \overline{U} + \overline{H_1} \overline{V} = \overline{1}$$

Pour calculer A et B , on effectue la division euclidienne de $\overline{C\overline{V}}$ par $\overline{G_1}$: $\overline{C\overline{V}} = \overline{G_1}\overline{Q} + \overline{A}$ avec $\deg(A) \leq r - 1$ et on prend $\overline{B} = \overline{U\overline{C}} + \overline{H_1}\overline{Q}$ de sorte que $\deg(B) \leq s - 1$.

Pour établir l'unicité, supposons que l'on ait d'autres polynômes $\widetilde{G}_n$ et $\widetilde{H}_n$ satisfaisant aux mêmes conditions. On a alors :

$$\begin{aligned}\widetilde{G}_n &= G_n + p^{n-1}M & \text{et} & \quad \deg(M) < \deg(\widetilde{G}_n) = \deg(G_n) \\ \widetilde{H}_n &= H_n + p^{n-1}N & \text{et} & \quad \deg(N) < \deg(\widetilde{H}_n) = \deg(H_n)\end{aligned}$$

de sorte que

$$\underbrace{\widetilde{G}_n \widetilde{H}_n}_{=F+p^n \tilde{P}} = \underbrace{G_n H_n}_{=F+p^n P} + p^{n-1}(G_n N + H_n M) + p^{2n-2}MN$$

Il en résulte que dans $K[X]$ on a

$$\overline{G_n N} + \overline{H_n M} = \overline{0}$$

Mais $\overline{G_n} = \overline{G_1}$ et $\overline{H_n} = \overline{H_1}$ sont premiers entre eux dans $K[X]$ de sorte que $\overline{M} = \overline{N} = \overline{0}$ et p divise M et N . Finalement on :

$$\widetilde{G}_n \equiv G_n \pmod{\mathbb{Z}[X]p^n} \text{ et } \widetilde{H}_n \equiv H_n \pmod{\mathbb{Z}[X]p^n}$$

Δ

On en déduit l'algorithme suivant :

Algorithme 2 (Relèvement de Hensel)

1. entrées :

(a) p premier

(b) $F, G, H \in \mathbb{Z}[X]$ tels que

i. F est unitaire

ii. $\overline{F} = \overline{G}.\overline{H}$ avec $\overline{G}$ et $\overline{H}$ unitaires et premiers entre eux dans $\mathbb{F}_p[X]$

iii. calculer les coefficients de Bezout U et V de G et H dans $\mathbb{F}_p[X] : GU + HV = 1$

(c) $n \geq 2$

2. boucle pour k variant de 2 à n :

{

(a) $C := (F - GH)/p^{k-1}$

(b) diviser dans $\mathbb{F}_p[X] : VC = GQ + A$ avec $\deg(A) < \deg(G)$

(c) $B := UC + QH \pmod{\mathbb{Z}[X]p}$

(d) $G := G + p^{k-1}A$

(e) $H := H + p^{k-1}B$

}

3. sorties : G, H tels que $F \equiv GH \pmod{\mathbb{Z}[X]p^n}$

Exemple :

On considère le polynôme :

$$F = X^9 + 4X^8 + X^7 + X^6 + X^5 + 2X^4 + 4X^3 + 3X^2 + 2 \in \mathbb{Z}[X]$$

On prend $p = 5$. Dans $\mathbb{F}_5[X]$, on a $\overline{F} = \overline{G_1} \overline{H_1}$ avec :

$$G_1 = X^3 + X^2 + 4X + 3 \quad \text{et} \quad H_1 = X^6 + 3X^5 + 4X^4 + 2X^3 + 4X^2 + 3X + 4$$

On a alors :

$G_2 = X^3 - 4X^2 + 9X + 8$	$H_2 = X^6 + 8X^5 - X^4 - 8X^3 - 11X^2 - 12X - 6$
$G_3 = X^3 + 21X^2 + 34X + 8$	$H_3 = X^6 - 17X^5 - 51X^4 + 17X^3 + 14X^2 + 38X - 31$
$G_4 = X^3 - 229X^2 + 284X - 242$	$H_4 = X^6 + 233X^5 - 51X^4 - 108X^3 - 111X^2 - 212X - 31$
$G_5 = X^3 - 1479X^2 + 1534X + 1008$	$H_5 = X^6 + 1483X^5 + 1199X^4 + 517X^3 - 736X^2 + 413X - 31$
$G_6 = X^3 + 4771X^2 - 4716X + 1008$	$H_6 = X^6 - 4767X^5 - 1926X^4 + 3642X^3 + 2389X^2 + 413X - 31$
$G_7 = X^3 + 36021X^2 - 35966X + 1008$	$H_7 = X^6 - 36017X^5 - 17551X^4 + 19267X^3 + 33639X^2 + 31663X - 15656$
$G_8 = X^3 + 36021X^2 - 114091X - 77117$	$H_8 = X^6 - 36017X^5 - 173801X^4 + 175517X^3 - 44486X^2 + 109788X + 140594$
$G_9 = X^3 + 426646X^2 - 504716X + 313508$	$H_9 = X^6 - 426642X^5 + 216824X^4 - 605733X^3 + 736764X^2 + 500413X - 250031$
$G_{10} = X^3 - 1526479X^2 + 1448409X - 3592742$	$H_{10} = X^6 + 1526483X^5 - 3689426X^4 + 3300517X^3 - 3169486X^2 + 500413X - 2203156$

On peut généraliser facilement à plusieurs facteurs¹⁰

3 Factorisation dans $\mathbb{Z}[X]$

3.1 Quelques inégalités.

Etant donné un polynôme $f = a_d X^d + \dots + a_1 X + a_0 \in \mathbb{C}[X]$ de degré d , on définit les normes :

$$\|f\|_1 = \sum_{i=0}^d |a_i| \quad , \quad \|f\|_\infty = \max(|a_0|, \dots, |a_d|) \quad \text{et} \quad \|f\|_2 = (|a_d|^2 + \dots + |a_1|^2 + |a_0|^2)^{\frac{1}{2}}$$

et la *mesure* de f :

$$M(f) = |a_d| \prod_{i=1}^d \max(1, |z_i|)$$

où $z_1, \dots, z_d \in \mathbb{C}$ sont les racines¹¹ de f .

Notons que l'on a $M(fg) = M(f)M(g)$ pour $f, g \in \mathbb{C}[X]$

Lemme 1 (*inégalité de Landau*)

Pour tout polynôme $f \in \mathbb{C}[X]$ on a :

$$M(f) \leq \|f\|_2$$

10. Soient un polynôme unitaire $F \in \mathbb{Z}[X]$ et p un entier premier tel que $\overline{F} \in \mathbb{F}_p[X]$ soit *sans facteurs multiples* ; considérons une factorisation $\overline{F} = \overline{F}_1 \dots \overline{F}_r$ dans $\mathbb{F}_p[X]$ avec les polynômes $\overline{F}_i$ unitaires deux à deux premiers entre eux. Alors, pour tout $n \geq 2$, il existe des polynômes unitaires $G_{n,i} \in \mathbb{Z}[X]$, $1 \leq i \leq r$, uniques modulo $\mathbb{Z}[X]p^n$ tels que :

- i. $F \equiv G_{n,1} \dots G_{n,r} \pmod{\mathbb{Z}[X]p^n}$ (on pose $G_{1,i} = F_i$ pour $1 \leq i \leq r$)
- ii. $G_{n,i} \equiv G_{n-1,i} \pmod{\mathbb{Z}[X]p^{n-1}}$

11. répétées avec leur ordre de multiplicité

▽ Supposons que $z_1, \dots, z_s$ soient les racines z de f telles que $|z| \leq 1$ de sorte que :

$$M(f) = |a_d| \prod_{i=1}^d \max(1, |z_i|) = |a_d| \prod_{i=s+1}^d |z_i|$$

La *formule de Jensen* s'écrit :

$$\operatorname{Log} \left| \frac{f(0)}{z_1 \cdots z_s} \right| = \frac{1}{2\pi} \int_0^{2\pi} \operatorname{Log} |f(e^{i\theta})| d\theta$$

On a $|a_0| = |a_d z_1 \cdots z_d|$ et $a_0 = f(0)$ d'où $\left| \frac{f(0)}{z_1 \cdots z_s} \right| = |a_d| |z_{s+1}| \cdots |z_d| = M(f)$ de sorte que :

$$\operatorname{Log} M(f) = \frac{1}{2\pi} \int_0^{2\pi} \operatorname{Log} |f(e^{i\theta})| d\theta$$

On a encore :

$$\operatorname{Log} M(f) = \frac{1}{2} \left(\frac{1}{2\pi} \int_0^{2\pi} \operatorname{Log} |f(e^{i\theta})|^2 d\theta \right)$$

Par ailleurs, puisque la fonction Log est *concave*, on a l'*inégalité de Jensen* :

$$\frac{1}{2\pi} \int_0^{2\pi} \operatorname{Log} |f(e^{i\theta})|^2 d\theta \leq \operatorname{Log} \left(\frac{1}{2\pi} \int_0^{2\pi} |f(e^{i\theta})|^2 d\theta \right)$$

Pour des polynômes f, g on considère le produit scalaire :

$$\langle f, g \rangle = \frac{1}{2\pi} \int_0^{2\pi} f(e^{i\theta}) \overline{g(e^{i\theta})} d\theta$$

pour lequel $(X^i)_{i \leq 0}$ est une *base orthonormée* de sorte que :

$$\frac{1}{2\pi} \int_0^{2\pi} \operatorname{Log} |f(e^{i\theta})|^2 d\theta = \langle f, f \rangle = |a_d|^2 + \cdots + |a_1|^2 + |a_0|^2 = \|f\|_2^2$$

et l'on a :

$$\operatorname{Log} M(f) \leq \frac{1}{2} \operatorname{Log} (\|f\|_2^2) = \operatorname{Log} \|f\|_2$$

d'où l'inégalité de Landau :

$$M(f) \leq \|f\|_2$$

On peut aussi démontrer l'inégalité de Landau élémentairement :

Lemme 2 Pour tout polynôme $g \in \mathbb{C}[X]$ et tout $z \in \mathbb{C}$ on a :

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

▽ Posons $g = \sum_{i=0}^e c_i X^i$. On a alors :

$$\begin{aligned} \|(X - z)g\|_2^2 &= |zc_0|^2 + \sum_{i=1}^e |c_{i-1} - zc_i|^2 + |c_e|^2 \\ &= |zc_0|^2 + \sum_{i=1}^e (|c_{i-1}^2 + |z|^2 |c_i|^2 - zc_i \overline{c_{i-1}} - \bar{z}c_{i-1} \overline{c_i}) + |c_e|^2 \\ &= (1 + |z|^2) \|g\|_2^2 - \sum_{i=1}^e (zc_i \overline{c_{i-1}} + \bar{z}c_{i-1} \overline{c_i}) \end{aligned}$$

On a alors

$$\begin{aligned}
\|(\bar{z}X - 1)g\|_2 &= |\bar{z}|^2 \left\| \left(X - \frac{1}{\bar{z}}\right)g \right\|_2^2 \\
&= |\bar{z}|^2 \left(\left(1 + \frac{1}{|\bar{z}|^2}\right) \|g\|_2^2 - \sum_{i=1}^e \left(\frac{1}{\bar{z}} c_i \overline{c_{i-1}} + \frac{1}{z} c_{i-1} \bar{c}_i\right) \right) \\
&= (1 + |z|^2) \|g\|_2^2 - \sum_{i=1}^e (z c_i \overline{c_{i-1}} + \bar{z} c_{i-1} \bar{c}_i) \\
&= \|(X - z)g\|_2^2
\end{aligned}$$

△

On déduit de ce lemme l'inégalité de Landau :

Soit s le plus grand indice tel que $|z_s| > 1$ de sorte que $M(f) = |a_n| \prod_{i=1}^s |z_i|$.

Considérons alors le polynôme :

$$g = a_n \prod_{i=1}^s (\bar{z}_i X - 1) \prod_{i=s+1}^d (X - z_i)$$

On a alors $\|f\|_2 = \|g\|_2 \geq |\text{lc}(g)| = M(f)$. △

Corollaire 1

On les inégalités :

$$\|f\|_\infty \leq \|f\|_2 \leq \|f\|_1 \leq (d+1) \|f\|_\infty \quad \text{et} \quad 2^{-d} \|f\|_1 \leq M(f) \leq \|f\|_2$$

▽ Le premier groupe reprend les inégalités sur les normes de $\mathbb{C}^{d+1}$. Par ailleurs on a les *relations entre coefficients et racines* :

$$a_{d-i} = (-1)^i a_d E_i(z_1, \dots, z_d) \text{ pour } 1 \leq i \leq d$$

où $E_1, \dots, E_d$ désignent les polynômes symétriques élémentaires en d indéterminées $X_1, \dots, X_d$.
On a :

$$\begin{aligned}
\|f\|_1 &= \sum_{i=0}^d |a_i| \\
&= |a_d| + \sum_{i=1}^d |a_{d-i}| \\
&\leq |a_d| \left(1 + \sum_{i=1}^d |E_i(z_1, \dots, z_d)|\right) \\
&\leq |a_d| \prod_{i=0}^d (1 + |z_i|) \\
&\leq |a_d| \prod_{i=0}^d 2 \max(1, |z_i|) \\
&\leq 2^d M(f)
\end{aligned}$$

La dernière relation étant l'inégalité de Landau. △

Corollaire 2 (borne de Mignotte)

Soient $f, g \in \mathbb{Z}[X]$ avec $g|f$; on pose $d = \deg(f)$; on a :

$$\|g\|_\infty \leq 2^d \|f\|_2 \leq 2^d (d+1) \|f\|_\infty$$

▽ Soit $e = \deg(g)$; si $f = gh$ on a :

$$\begin{aligned}
\|g\|_\infty \|h\|_\infty &\leq \|g\|_1 \|h\|_1 \\
&\leq 2^e M(f) 2^{d-e} M(h) \\
&\leq 2^d M(f) \\
&\leq 2^d \|f\|_2 \\
&\leq 2^d (d+1) \|f\|_\infty
\end{aligned}$$

△

3.2 Factorisation dans $\mathbb{Z}[X]$

On considère un polynôme *unitaire*¹² *sans facteur multiple*¹³ $f \in \mathbb{Z}[X]$. On détermine alors un entier premier p *impair* tel que la réduction $\bar{f}$ de f *modulo* p reste sans facteur multiple¹⁴. On factorise¹⁵ alors $\bar{f}$ dans $\mathbb{Z}/p\mathbb{Z}[X]$.

On choisit ensuite une borne¹⁶ B pour les coefficients des facteurs g de f puis le plus petit exposant n tel que $p^n > 2B$.

On utilise la représentation *symétrique* des éléments de $\mathbb{Z}/\mathbb{Z}p^n$ *i.e.* on prend comme système de représentants l'intervalle entier $[-\frac{p^n-1}{2}, \frac{p^n-1}{2}]$, ainsi les coefficients b_j d'un diviseur g de f *s'écrivent de la même manière* dans $\mathbb{Z}$ et dans $\mathbb{Z}/\mathbb{Z}p^n$ puisque que l'on a $|b_j| \leq B \leq \frac{p^n-1}{2}$.

On construit alors le relèvement de Hensel dans $\mathbb{Z}/p^n\mathbb{Z}[X]$ de la factorisation précédente et l'on obtient donc $f \equiv P_1 \cdots P_r \pmod{p^n}$.

Enfin on *essaie* des combinaisons $P_{j_1} \cdots P_{j_k}$ jusqu'à obtenir une factorisation complète de f .

Algorithme 3 (Factorisation de Zassenhaus)

1. *entrée* : $f \in \mathbb{Z}[X]$ *sans facteur multiple*
2. *calculer* p *premier tel que* $\bar{f}$ *soit sans facteur multiple dans* $\mathbb{F}_p$
3. *calculer une borne* B *pour les coefficients des facteurs de* f
4. *calculer le plus petit entier* n *tel que* $p^n > 2B$
5. *factoriser* $f \pmod{p}$. On a $\bar{f} = \bar{F}_1 \cdots \bar{F}_N$
6. *former l'ensemble* $\mathfrak{P}(\{1, \dots, N\})$ *des parties de* $\{1, \dots, N\}$ *d'au plus* $\frac{N}{2}$ *éléments*
7. *pour* S *parcourant* $\mathfrak{P}(\{1, \dots, N\})$, *boucle* :
 - (a) *prendre* $G = \prod_{i \in S} F_i$ *et* $H = \prod_{i \notin S} F_i = F/G$
 - (b) *calculer le relèvement de Hensel* (G_n, H_n) *dans* $\mathbb{Z}/\mathbb{Z}p^n[X]$ *de la factorisation* $\bar{F} = \bar{G}\bar{H}$.
 - (c) *si* G_n *divise* F *dans* $\mathbb{Z}[X]$ *mémoriser (dans une liste) la factorisation* $(G_n, F/G_n)$ *obtenue*
8. *sortie* : *la liste des facteurs de* f *dans* $\mathbb{Z}[X]$.

12. On ramène le cas d'un polynôme *primitif* $f \in \mathbb{Z}[X]$ de degré d et de coefficient dominant a au cas du polynôme *unitaire* $\tilde{f} = a^{d-1}f(\frac{1}{a}X)$. Si l'on a une factorisation $\tilde{f} = g.h$, on a $a^{d-1}f = g(dX)h(dX)$ et il suffit de considérer les parties primitives des deux membres

13. comme f est primitif il revient au même qu'il soit sans facteur multiple dans $\mathbb{Q}[X]$.

14. *ie.* tel que $\text{pgcd}(\bar{f}, \bar{f}') = \bar{1}$. Cela revient à ce que p ne divise pas le *discriminant* Δ de f . Comme f n'a pas de racine multiple on a $\Delta \neq 0$. Remarquons de plus que, d'après le *théorème de Hermite-Minkowski* on a $\Delta \neq \pm 1$.

15. par exemple à l'aide de l'algorithme de Berlekamp

16. grâce à la borne de Mignotte

Exemple :

On considère le polynôme $X^8 + 7X^7 + 9X^6 + 55X^5 + 8X^4 + 35X^3 - 86X^2 - 27X - 2 \in \mathbb{Z}[X]$; son discriminant est $\Delta = 2^4 \cdot 3^{18} \cdot 5 \cdot 7^3 \cdot 73^2 \cdot 1399$. On peut prendre $p = 11$ pour que $\overline{F} \in \mathbb{F}_{11}[X]$ soit sans facteur multiple. Une borne pour les coefficients des diviseurs de F est $B = 7910$ et on a alors $n = 5$. Les facteurs irréductibles de $\overline{F} \in \mathbb{F}_{11}[X]$ sont :

$$X - 4, X - 1, X + 3, X + 4, X + 5, X^3 - 4X + 1$$

Leurs relèvements de Hensel dans $\mathbb{Z}/p^n\mathbb{Z}[X]$ sont :

$$X + 78393, X - 1, X + 70656, X - 70649, X - 78392, X^3 + 7X + 1$$

Parmi ceux-ci, *lus dans* $\mathbb{Z}[X]$:

$$X - 1, X^3 + 7X + 1$$

sont des facteurs irréductibles de F . Il faut ensuite *tester des regroupements des polynômes restants* :

$$X + 78393, X + 70656, X - 70649, X - 78392$$

Les produits dans $\mathbb{Z}/p^n\mathbb{Z}[X]$ *lus dans* $\mathbb{Z}[X]$:

$$(X + 78393)(X - 78392) = X^2 + X + 2 \quad \text{et} \quad (X + 70656)(X - 70649) = X^2 + 7X + 1$$

sont les autres facteurs irréductibles de F .