UFR Sciences
M2 Calcul Formel
Option Maths approfondies

2012–2013
M. WEIMANN

Factorisation dans $\mathbb{Z}[x]$

Nous allons maintenant nous intéresser au problème de la factorisation des polynômes à coefficients dans $\mathbb{Z}$. L'objectif de ce chapitre est de développer un algorithme qui, étant donné $F \in \mathbb{Z}[x]$, retourne la liste $[(F_1, m_1), \ldots, (F_s, m_s)]$ des paires (facteurs irréductibles, multiplicités). L'idée générale est la suivante :

1. Factoriser modulo un "bon" premier $p \in \mathbb{N}$.
2. Remonter cette factorisation modulo p^k pour une précision k suffisamment grande.
3. Recombiner les facteurs modulaires dans $\mathbb{Z}/p^k\mathbb{Z}[x]$ en des facteurs dans $\mathbb{Z}[x]$.

Deux questions essentielles se posent :

1. Comment remonter une factorisation modulo p à une factorisation modulo p^k ? Le Lemme de Hensel répondra à cette question.

2. Quelle précision k faut-il choisir ? La borne de Mignotte-Landau des coefficients des facteurs répondra à cette question.

1 La remontée de Hensel

On se place ici dans le cadre général d'un polynôme univarié $F \in A[x]$ à coefficient dans un anneau commutatif A avec unité 1. On se fixe $m \in A$ et on suppose donnés deux polynômes G et H de $A[x]$ tels que

$$F \equiv GH \mod m, \quad Res(G, H) \neq 0 \mod m. \tag{1}$$

Le but est de remonter cette factorisation modulo (m) en une factorisation modulo (m^2), c'est à dire trouver $\hat{G}$ et $\hat{H}$ dans $A[x]$ congrus respectivement à G et H modulo (m) et tels que

$$F \equiv \hat{G}\hat{H} \mod m^2. \tag{2}$$

En itérant ce procédé, on obtiendra une factorisation modulo (m^k) pour k arbitrairement grand.

L'ingrédient clé est l'utilisation des *relations de Bezout* : puisque G et H sont supposés premiers entre eux modulo m, il existe deux polynômes U et V de $A[x]$ tels que

$$UG + VH \equiv 1 \mod m. \tag{3}$$

Lorsque $A/(m)$ est un corps, on peut calculer U et V grâce à l'*algorithme d'Euclide étendu* dans $A[x]/(m)$.

Proposition 1 *Une solution de l'équation (2) est donnée par*

$$\hat{G} = G + VE \quad \text{et} \quad \hat{H} = H + UE, \quad \text{avec} \quad E = F - GH$$

Preuve. On a les relations suivantes :

$$\begin{aligned} F - \hat{G}\hat{H} &= F - (G + VE)(H + UE) \\ &= F - GH - (UG + VH)E - UVE^2 \\ &= E(1 - (UG + VH)) - UVE^2. \end{aligned}$$

Par hypothèse, on a $E \equiv 0 \mod m$ et $UG + VH \equiv 1 \mod m$. Il suit que $F - \hat{G}\hat{H} \equiv 0 \mod m^2$. □

Deux inconvénients :

1. Les degrés de $\hat{G}$ et $\hat{H}$ ainsi définis peuvent être strictement supérieur à ceux de G et H. En particulier, on peut avoir $\deg(\hat{G}\hat{H}) > \deg(F)$ ce qui n'est pas très satisfaisant pour notre problème de factorisation.

2. Si on veut continuer de remonter la factorisation $\mod m^4$, etc..., on a besoin à chaque étape de calculer une relation de Bezout modulo une puissance de m. Plutôt que de recalculer cette relation à chaque étape, on va remonter la relation (3) de Bezout initiale modulo (m) en une relation de Bezout modulo (m^2), puis modulo (m^4), etc.

L'ingrédient clé est d'utiliser la division euclidienne (des polynômes unitaires) dans $A[x]$. On aura besoin du lemme suivant :

Lemme 1 *Soient S et T dans $A[x]$ avec T unitaire. Soient Q et R le quotient et le reste de la division de S par T. Si $S \equiv 0 \mod m$ alors*

$$Q \equiv 0 \mod m \quad \text{et} \quad R \equiv 0 \mod m$$

Preuve. Par hypothèse, il existe $\hat{S} \in A[x]$ tel que $S = m\hat{S}$. Soit

$$\hat{S} = \hat{Q}\,T + \hat{R} \quad \text{avec} \quad \deg \hat{R} < \deg T$$

la division avec reste de $\hat{S}$ par T. Alors $S = m\hat{Q}\,T + m\hat{R}$, avec $\deg(m\hat{R}) < \deg T$. Comme le quotient et le reste sont uniques, il suit que $Q = m\hat{Q}$ et $R = m\hat{R}$. □

On peut maintenant montrer la proposition centrale de cette section :

Proposition 2 *Soient $F \in A[x]$ et $m \in A$ fixés. Supposons donnés G, H, U, V dans $A[x]$ tels que*

- $F \equiv GH \mod m$ *avec H unitaire et* $\deg G + \deg H = \deg F$.
- $UG + VH \equiv 1 \mod m$, *avec* $\deg U < \deg H$ *et* $\deg V < \deg G$.

Alors il existe $\hat{G}, \hat{H}, \hat{U}, \hat{V}$ dans $A[x]$ congrus à G, H, U, V modulo m et tels que

- $F \equiv \hat{G}\hat{H} \mod m^2$ *avec $\hat{H}$ unitaire et* $\deg \hat{G} + \deg \hat{H} = \deg F$.
- $\hat{U}\hat{G} + \hat{V}\hat{H} \equiv 1 \mod m^2$, *avec* $\deg \hat{U} < \deg \hat{H}$ *et* $\deg \hat{V} < \deg \hat{G}$.

Preuve. La preuve est constructive. On va utiliser des divisions euclidiennes dans l'anneau $A[x]$:pour S, T deux polynômes avec T unitaire, on note

$$(Q, R) := \mathrm{Div}(S, T)$$

le couple (quotient, reste) de la division de S par T (comme A n'est a priori pas un corps, T doit être supposé unitaire pour que la division euclidienne de S par Q ait un sens dans $A[x]$). On définit :

$$E := F - GH \mod m^2 \quad \text{et} \quad (Q, R) := \mathrm{Div}(UE, H) \mod m^2$$

et on pose

$$\hat{G} := G + VE + QG \mod m^2 \quad \text{et} \quad \hat{H} := H + R \mod m^2$$

Comme $E \equiv 0 \mod m$, on a :

$$\begin{aligned} F - \hat{G}\hat{H} &\equiv F - (G + VE + QG)(H + UE - QH) \mod m^2 \\ &\equiv F - GH - GUE + VEH - VEQH + QGUE - Q^2HG \mod m^2 \\ &\equiv E(1 - (GU + VH)) + QE(GU - VH) - Q^2HG \mod m^2 \end{aligned}$$

Comme $UE \equiv QH + R$. Comme $E \equiv 0 \mod m$, il suit du Lemme 1 que $Q \equiv 0 \mod m$. Comme de plus $GU + VH \equiv 1 \mod m$, il suit finalement que

$$F - \hat{G}\hat{H} \equiv 0 \mod m^2.$$

De plus, il suit que

$$\hat{G} \equiv G + VE + QG \equiv G \mod m \quad \text{et} \quad \hat{H} \equiv H + UE - QH \equiv H \mod m.$$

Finalement, comme H est supposé unitaire et $\deg R < \deg H$, on a $\hat{H} = H + R$ unitaire aussi.

Concernant la relation de Bezout, on définit cette fois

$$B := U\hat{G} + V\hat{H} - 1 \mod m^2 \quad \text{et} \quad (C, D) := \mathrm{Div}(UB, \hat{H}) \mod m^2$$

et on pose

$$\hat{U} := U - D \mod m^2 \quad \text{et} \quad \hat{V} := V(1 - B) - C\hat{G} \mod m^2.$$

On montre alors avec le même type d'arguments que le couple $(\hat{U}, \hat{V})$ donne la relation de Bezout modulo m^2 recherchée. □

Etant donné $F \in \mathbb{Z}[x]$ unitaire sans facteurs multiples (discriminant non nul) et p un premier tel que F reste sans facteurs irréductibles modulo (p) (*i.e* p ne divise pas le discriminant), la Proposition 2 va nous permettre de relever la factorisation de F modulo p en une factorisation modulo p^2, puis p^4, etc, jusqu'à une précision arbitrairement grande fixée. Reste maintenant à savoir quelle précision est suffisante pour retrouver les facteurs de F sur $\mathbb{Z}$.

2 Majoration des coefficients des facteurs

Soit $F \in \mathbb{Z}[x]$ et Q un facteur de F. Le but de cette section est de trouver une borne sur la taille des coefficients de Q en fonction des coefficients de F. On introduit pour cela deux manières de mesurer la "taille" d'un polynôme.

Définition 1 *Soit $F \in \mathbb{C}[x]$ un polynôme à coefficients complexes :*

$$F(x) = a_n x^n + \cdots + a_1 x + a_0.$$

On appelle ***norme*** *de F le réel positif*

$$\|F\| := \sqrt{|a_0|^2 + \cdots + |a_n|^2}.$$

On appelle ***mesure*** *de F le réel ≥ 1*

$$M(F) := |a_n| \prod_{i=1}^{n} \max\big(1, |z_i|\big).$$

où $z_1, \ldots, z_n$ sont les racines de F (pas nécessairement distinctes).

L'un des intérêts de la mesure est d'être multiplicative

$$M(GH) = M(G)M(H)$$

et de fournir une majoration des coefficients :

Proposition 3 Soit F un polynôme comme ci-dessus. On a

$$\max |a_j| \leq \binom{n}{[n/2]} M(P), \quad \forall\, i = 0, \ldots, n$$

Preuve. Cela résulte de l'expression des coefficients d'un polynôme comme fonctions symétriques des racines :

$$a_{n-j} = (-1)^{n-j} a_n \sum_{1 \leq k_1 < < k_j \leq n} z_{k_1} \cdots z_{k_j}.$$

On obtient $|a_{n-j}| \leq \binom{n}{j} M(F)$, d'où l'assertion. □

Reste maintenant à donner une majoration aisément calculable de $M(F)$.

Proposition 4 *Pour tout nombre complexe z, on a*

$$\|(x - z)F\| = \|(\bar{z}x - 1)F\|$$

Preuve. On utilisant l'égalité

$$\int_0^{2\pi} e^{kit} dt = \begin{cases} 0 & \text{si} \quad k \neq 0 \\ 2\pi & \text{si} \quad k = 0 \end{cases}$$

on déduit aisément l'égalité

$$\|Q\|^2 = \frac{1}{2\pi} \int_0^{2\pi} |Q(e^{it})|^2 dt.$$

pour tout $Q \in \mathbb{C}[x]$. Il suffit alors de poser $Q = (x - z)F$ et de remarquer que $|e^{it} - z| = |e^{-it} - \bar{z}| = |1 - \bar{z}e^{it}|$. □

Théorême 1 *(inégalité de Mignotte-Landau) On a l'inégalité :*

$$M(F) \leq \|F\|.$$

Preuve. Soit $I \subset \{1, \ldots, n\}$ l'ensemble des indices tels que $|z_i| > 1$. Ainsi,

$$M(F) = |a_n| \prod_{i \in I} |z_i|.$$

Considérons alors le polynôme :

$$Q(x) = \prod_{i \in I} (\bar{z}_i x - 1) \times \prod_{i \notin I} (x - z_i)$$

Une application répétée du lemme précédant donne

$$\|F\| = \|Q\|$$

Par construction, on a $M(F) = lc(Q)$, où $lc(Q)$ désigne le coefficient dominant de Q. On conclut avec l'inégalité $|lc(Q)| \leq \|Q\|$. □

Corollaire 1 *Si G est un facteur de degré k de F alors $\|G\| \leq \binom{k}{[k/2]} \|F\|$.*

Preuve. Il suffit de combiner les résultats précédants, en remarquant que $M(G) \leq M(F)$. □

3 L'algorithme

On a maintenant tous les ingrédients pour donner un algorithme de factorisation d'un polynôme $F \in \mathbb{Z}[x]$.

Etape 1. *Rédution au cas unitaire.* Pour se ramener au cas unitaire, on calcule d'abord le *contenu* $c(F)$ de F (pgcd des coefficients de F), puis on divise F par $c(F)$ pour se ramener au cas d'un polynôme *primitif* ($c(F) = 1$). Si a est le coefficient dominant d'un polynôme primitif F de degré n, le polynôme

$$\tilde{F}(x) := a^{n-1} F(x/a)$$

est dans $\mathbb{Z}[x]$, unitaire de degré n. De plus, si l'on a une factorisation $\tilde{F} = GH$, on retrouve la factorisation de F correspondante à l'aide de l'identité $a^{n-1}F = G(aX)H(aX)$ et en considérant la partie primitive des deux membres.

Etape 2. *Rédution au cas sans facteurs multiples.* On calque la méthode décrite dans le cas de $\mathbb{F}_p$. Puisque la caractéristique est nulle ici, on a $F' \neq 0$ et il suffit de remplacer F par $\text{pgcd}(F, F')$. On trouve ensuite les multiplicités par pgcd ou résultants successifs.

Etape 3. *Factorisation modulo un bon p.* On choisit un nombre premier p tel que $F \mod p$ reste sans facteurs multiples dans $\mathbb{F}_p[x]$. Pour ce faire, il suffit de choisir pour p un nombre premier ne divisant pas le résultant de F et F' (ou, mieux, un nombre premier ne divisant pas le discriminant

de F). Certainement, un facteur G de F est aussi un facteur de F modulo p ($G \mod p$ n'étant pas nécessairement irréductible, même si G l'est). On factorise donc $F \mod p$ sur $\mathbb{F}_p[x]$,

$$F = G_1 \times \cdots \times G_r \mod p,$$

avec les G_i irréductibes dans $\mathbb{F}_p[x]$ et distincts deux à deux.

Etape 4. *Remontée de Hensel à la bonne précision.* Si le polynôme F de degré n n'est pas irréductible, il a un facteur G de degré inférieur ou égal à $n/2$. Par la borne de Mignotte-Landau, les valeurs absolues des coefficients de G sont donc majorées par $N := \binom{[n/2]}{[n/4]}\|F\|$. On prend donc un nombre entier k tel que $p^k > 2N$ et on réitère le lemme de Hensel pour remontée la factorisation modulo p en une factorisation

$$F = \hat{G}_1 \times \cdots \times \hat{G}_r \mod p^k$$

Puisque la précision double à chaque fois, le nombre d'itérations nécessaires est de l'ordre de $\log_2(N/log(p))$. Si l'on prend comme représentants des éléments de $\mathbb{Z}/p^k\mathbb{Z}$ les nombres entiers dans l'intervalle $[-p^k/2, p^k/2]$, vue l'unicité de la factorisation modulo p^k et la borne sur les coefficients de G, nécessairement G coïncidera avec le produit de certains des $\hat{G}_i$.

Etape 5. *Recombinaisons.* Ainsi, il suffit de regarder les partitions $I \cup J$ de $\{1, \ldots, r\}$, de poser

$$A = \prod_{i \in I} \hat{G}_i \quad \text{et} \quad B \prod_{i \in J} \hat{G}_i.$$

Si aucun des polynômes A ou B n'a de facteurs commun avec F, on change de partition. Si l'on a épuisé toutes les partitions, F est irréductible. Sinon, on a trouvé une factorisation $F = GH$. Puis on réitère l'étape 5 pour factoriser G, puis H.

Remarque 1 Il s'avère en pratique que la borne de Mignotte-Landau est souvent pessimiste et que l'on peut arréter la remontée de Hensel à une précision moindre pour récupérer certains facteurs. Une astuce : si un facteur modulaire ne change pas lors d'une étape de la remontée de Hensel, il est probable que ce soit un facteur de F. On teste donc son pgcd avec F pour s'en assurer. Si par exemple $F = (x^2 + 1)(100000x^5 + 2540153x^4 + ...)$, le premier facteur sera détecté et calculé très vite.

Remarque 2 La méthode des recombinaisons des facteurs modulaires est aussi employée pour factoriser les polynômes à deux variables dans $\mathbb{Q}[t, x] = \mathbb{Q}[t][x]$. Cette fois, on regarde la factorisation modulo (t) (par exemple en utilisant l'algorithme précédant). On la remonte modulo (t^k) pour k suffisamment grand grâce au Lemme de Hensel, puis on recombine les facteurs modulaires. La borne de Mignotte-Landau est cette fois remplacée par le degré en t de F. Une différence notoire avec le cas $\mathbb{Z}[x]$ est qu'il est possible de réduire le problème des recombinaisons des facteurs modulaires à de l'algèbre linéaire, évitant ainsi de tester le nombre exponentiel de partitions de l'ensemble des facteurs modulaires, étape coûteuse quand le polynôme a beaucoup de facteurs modulo p.

Remarque 3 Mentionnons pour finir une autre approche conduisant de la factorisation des polynômes à coefficients entiers ; l'algorithme LLL de réduction des réseaux permet de reconstruire les polynômes minimaux des racines de F (donc des facteurs irréductibles) à partir d'approximations convenables de ces dernières.

4 Factorisation sur $\mathbb{Z}[x]$: Exercices et TP

Objectif : Illustrer les diverses étapes de la factorisation sur $\mathbb{Z}[x]$ décrites dans le cours en implémentant et testant quelques uns des algorithmes sous-jacents. Le but ultime serait de développer un algorithme de factorisation complet sur $\mathbb{Z}[x]$ qui utilise la factorisation sur $\mathbb{F}_p$, mais ce serait a priori un peu trop gourmand pour un oral d'aggregation. Voici quelques exercices guides...

Exercice 1 Ecrire une procédure **Hensel**(F, G, H, U, V, p, k) qui, étant donnés $F, G, H, U, V \in \mathbb{Z}[x]$, p premier et $k \in \mathbb{N}$ satisfaisant

- $F \equiv GH \mod p$ avec H unitaire et $\deg\ G + \deg\ H = \deg\ F$,
- $UG + VH \equiv 1 \mod p$, avec $\deg\ U < \deg\ H$ et $\deg\ V < \deg\ G$,

retourne $\hat{G}, \hat{H}, \hat{U}, \hat{V}$ dans $\mathbb{Z}[x]$ égaux à G, H, U, V modulo p et tels que

- $F \equiv \hat{G}\hat{H} \mod p^{2^k}$ avec $\hat{H}$ unitaire et $\deg\ \hat{G} + \deg\ \hat{H} = deg\ F$,
- $\hat{U}\hat{G} + \hat{V}\hat{H} \equiv 1 \mod (p^{2^k})$, avec $\deg\ \hat{U} < \deg \hat{H}$ et $\deg \hat{V} < \deg \hat{G}$,

On pourra utiliser une sous-procédure **EtapeHensel** traitant la cas $k = 1$, que l'on itérera pour généraliser à tout k.

Exercice 2 Ecrire une procédure **Precision**(F,p) qui retourne le nombre d'itérations de la remontée de Hensel des facteurs modulo (p) qui sont nécessaires pour atteindre la borne de Mignotte-Landau des coefficients des facteurs de F sur $\mathbb{Z}[x]$.

Exercice 3 En déduire une procédure **FactoModulaire**(F, p, k) qui, étant donnés $F \in \mathbb{Z}[x]$ unitaire, p premier et $k \in \mathbb{N}$ retourne *Faux* si F n'est pas réduit (sans facteurs carrés) modulo p et retourne la factorisation de F modulo (p^k) sinon (sous forme de liste).

Exercice 4 Ecrire une procédure **Recombinaisons**(F, p, k) qui étant donnés $F \in \mathbb{Z}[x]$ unitaire, p premier et $k \in \mathbb{N}$ retourne l'ensemble des facteurs irréductibles de F pouvant s'obtenir comme produit d'éléments de la liste **FactoModulaire**(F, p, k). Il faut utiliser la fonction $set-partitions(S, 2)$ de Maxima offrant toutes les partitions d'un ensemble S en deux sous-ensembles disjoints. On peut essayer de l'ordonner intelligemment en utilisant la fonction de tri *sort*.

Exercice 5 Ecrire une procédure **FactoUnitaire**(F,n) qui, donnés $F \in \mathbb{Z}[x]$ et $n \in \mathbb{N}$, retourne **Faux** si F n'est pas unitaire sans facteurs carrés, et retourne la liste des facteurs irréductibles de F sinon. On utilisera une factorisation modulo des puissances de p, où p est le plus petit premier supérieur ou égal à n pour lequel F est réduit modulo p. On pourra inclure l'affichage de p, l'affichage de la borne de Mignotte-Landau N, et les temps des sous-procédures **FactoModulaire**(F, p,N) et **Recombinaisons**(F, p, N), puis le temps total de **FactoUnitaire**(F,n).

Exercice 6 Ecrire une procédure **Factorisation**(F) qui, donné $F \in \mathbb{Z}[x]$ quelconque, retourne sa factorisation irréductible sous la forme d'une liste

$$L(F,p) = [c, (F_1, m_1), \ldots, (F_s, m_s)],$$

avec c le contenu de F et où les couples (F_i, m_i) sont consitués des facteurs irréductibles de F et de leurs multiplicités.

Exercice 7 Ecrire une variante permettant de détecter les facteurs de petits coefficients au cours de la remontée de Hensel. Comparer l'algorithme précédant et sa variante sur des exemples.

Exercice 8 Autres suggestions... Inclure des compteurs temps dans les différentes sous-procédure de **Factorisation**(F). Créer des tableaux de valeurs "temps de Hensel", "temps des recombinaisons". Remplir ce tableaux avec un échantillonage significatif de polynÃťmes. Regarder les comportements du temps d'exécution en fonction du degré, du nombre de facteurs modulaires, du premier p, etc..(éventuellement en traçant des courbes).