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

HOSSAIN Akash,
NGUYEN Elise

Introduction

Le problème de factorisation dans $\mathbb{Z}[X]$ peut s'exprimer de la manière suivante :

Entrée : $P \in \mathbb{Z}[X] \setminus \{0\}$.

Sortie : Un ensemble de couples (les facteurs et leur multiplicité) $E \subset \mathbb{Z}[X] \times \mathbb{N}^*$, et un inversible $F \in \mathbb{Z}[X]^*$ tels que :

- Pour tout $(Q,\ m)$, $(Q',\ m') \in E$, si Q et Q' sont associés, alors $(Q,\ m) = (Q',\ m')$. (il n'y a pas de redondance des facteurs)
- Pour tout $(Q,\ m) \in E$, Q est irréductible.
- $P = F \times \prod_{(Q,\ m) \in E} Q^m$.

Remarques

- L'anneau $\mathbb{Z}[X]$ est factoriel, donc la solution existe toujours.
- Nous allons élargir l'ensemble qui contient F à $\mathbb{Z}$. Nous considérerons ainsi que des polynômes comme 4 sont irréductibles, même si ce n'est pas le cas. Pour avoir une factorisation complète, il faut savoir factoriser dans $\mathbb{Z}$, et c'est un tout autre problème que nous n'aborderons pas.

Pour cela, nous allons d'abord factoriser notre polynôme dans un corps premier fini avec l'algorithme de Berlekamp, puis nous utiliserons la remontée de Hensel pour déduire d'une factorisation dans $\mathbb{F}_p[X]$ une factorisation dans $\mathbb{Z}[X]$.

1 Premières simplifications

Nous allons montrer comment réduire le problème de factorisation d'un polynôme quelconque à un problème de factorisation sur un polynôme sans facteur multiple (toutes les multiplicités valent 1).

Définitions et propriétés

Pour $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$, le **contenu** de P est $c(P) = pgcd_{i=0}^{n}(a_i)$, qui peut être vu comme le plus grand entier naturel qui divise P.

On dit alors que P est **primitif** quand $c(P) = 1$.

Théorème Le produit de deux polynômes primitifs est primitif.

Preuve Soient P et Q des polynômes primitifs. Supposons par l'absurde que $c(PQ)$ n'est pas associé à 1. Soit p un diviseur premier de $c(PQ)$. p divise PQ, donc pour π la surjection canonique $\mathbb{Z}[X] \to \mathbb{Z}[X]/(p)$, on a $\pi(P)\pi(Q) = \pi(PQ) = 0$. Or, $\mathbb{Z}[X]/(p)$ est isomorphe à l'anneau intègre $\mathbb{F}_p[X]$. Donc $\pi(P) = 0$ ou $\pi(Q) = 0$, c'est à dire que p divise $c(P)$ ou $c(Q)$. C'est absurde, car P et Q sont primitifs. Ainsi, PQ est primitif.

Corollaire Pour P et Q dans $\mathbb{Z}[X]$, $c(PQ) = c(P)c(Q)$.

Preuve P peut s'écrire $c(P)P'$, avec P' un polynôme primitif. De même, $Q = c(Q)Q'$. Alors $PQ = c(P)c(Q)R$, avec $R = P'Q'$ un polynôme primitif. Il est ensuite clair que $c(c(P)c(Q)R) = c(P)c(Q)$.

Corollaire Les diviseurs d'un polynôme primitif sont tous primitifs.

1.1 Se ramener au cas primitif

Soit $P \in \mathbb{Z}[X]$. Il est assez clair qu'une factorisation de $\frac{1}{c(P)}P$ donnera immédiatement celle de P. Si E et F sont la solution du problème de factorisation présenté dans l'introduction, appliqué à $\frac{1}{c(P)}P$, alors E et $c(P)F$ seront la solution du problème appliqué à P.

1.2 Se ramener au cas unitaire

On veut factoriser $P = \sum_{i=0}^{n} a_i X^i$ un polynôme primitif.

Une simplification est de factoriser $a_n^{n-1}P(X/a_n) = \sum_{i=0}^{n} a_i a_n^{n-i-1} X^i = X^n + a_{n-1}X^{n-1} + a_n a_{n-2}X^{n-2} + ... + a_n^{n-1}a_0$, qui est un polynôme unitaire. En effet, si $a_n^{n-1}P(X/a_n) = \prod_{(Q,\, m)\in E} Q^m$, avec E vérifiant les critères de l'introduction (on ne note pas F le facteur entier, car F vaut 1), alors pour

$E' = \left\{ \left(\frac{1}{c(Q(a_n X))} Q(a_n X),\ m \right) | (Q,\ m) \in E \right\}$ on a $P = \prod_{(Q,\ m) \in E'} Q^m$, et E' vérifie les critères de l'introduction.

Preuve Soit $\phi : \mathbb{Z}[X] \to \mathbb{Z}[X]$, qui à Q associe $Q(a_n X)$. On rappelle que ϕ est un endomorphisme d'anneaux : c'est l'homomorphisme d'évaluation induit (par la propriété universelle des polynômes) par la restriction canonique $\mathbb{Z} \to \mathbb{Z}[X]$, et le polynôme du codomaine $a_n X \in \mathbb{Z}[X]$.

Montrons qu'il n'y a pas de redondance de facteurs dans E'. On remarque ϕ préserve le degré. Donc son noyau est nul et ϕ est **injective**. Par conséquent, si $\left(\frac{1}{c(\phi(Q))} \phi(Q),\ m \right)$ et $\left(\frac{1}{c(\phi(Q'))} \phi(Q'),\ m' \right)$ sont dans E', alors par injectivité de ϕ, si $\frac{1}{c(\phi(Q))} \phi(Q)$ et $\frac{1}{c(\phi(Q'))} \phi(Q')$ sont associés, on a $Q = Q'$. En effet, soit x un inversible tel que $\frac{1}{c(\phi(Q))} \phi(Q) = \frac{x}{c(\phi(Q'))} \phi(Q')$. On remarque que x est de degré 0, et $\phi(x) = x$. On a alors $\phi(Q) = \phi\left(\frac{x c(\phi(Q))}{c(\phi(Q'))} Q' \right)$ [1], c'est à dire $Q = \frac{x c(\phi(Q))}{c(\phi(Q'))} Q'$. En tant que diviseur d'un polynôme unitaire, Q est unitaire. Comme Q' est unitaire, $Q = Q'$. Comme E vérifie les critères de l'introduction, $m = m'$. Il n'y a pas de redondance de facteurs.

Montrons que $P = \prod_{(Q,\ m) \in E'} Q^m$.

L'idée est que $\phi\left(\prod_{(Q,\ m) \in E} Q^m \right) = \phi(a_n^{n-1} P(X/a_n)) = a_n^{n-1} P(a_n (X/a_n)) = a_n^{n-1} P$.

Donc, sachant que P est primitif,
$$\begin{aligned} P &= \frac{1}{c(a_n^{n-1} P)} a_n^{n-1} P \\ &= \frac{1}{\prod_{(Q,\ m) \in E} c(\phi(Q))^m} \phi\left(\prod_{(Q,\ m) \in E} Q^m \right) \\ &= \prod_{(Q,\ m) \in E} \left(\frac{1}{c(\phi(Q))} \phi(Q) \right)^m \\ &= \prod_{(Q,\ m) \in E'} Q^m. \end{aligned}$$

Soit $(Q,\ m) \in E$. Montrons que $\frac{1}{c(\phi(Q))} \phi(Q)$ est irréductible. La démonstration sera presque complète, et devrait donner une bonne idée de comment

1. Si l'on n'est pas convaincu que ce polynôme est dans $\mathbb{Z}[X]$, on peut étendre ϕ à $\mathbb{Q}[X]$, et l'injectivité sera conservée.

procéder. Par l'absurde, soient Q_1 et Q_2 deux polynômes non inversibles tels que $Q_1 Q_2 = \frac{1}{c(\phi(Q))}\phi(Q)$. Alors, pour $d_1 = deg Q_1$, et $d_2 = deg Q_2$, les polynômes $Q_1' = a_n^{d_1} Q_1(X/a_n)$ et $Q_2' = a_n^{d_2} Q_2(X/a_n)$ sont à coefficients dans $\mathbb{Z}$, et on a :

$$\phi(Q_1' Q_2') = a_n^{deg Q} Q_1 Q_2.$$

En multipliant par $c(\phi(Q))$ des deux côtés et en se servant de l'injectivité de ϕ, on obtient :

$$c(\phi(Q)) Q_1' Q_2' = a_n^{deg Q} Q$$

c'est à dire :

$$c(\phi(Q)) Q_1(X/a_n) Q_2(X/a_n) = Q.$$

Cela ne suffira pas à conclure rigoureusement la démonstration, mais l'idée est ensuite d'écrire $c(\phi(Q)) = n_1 n_2$, tel que $n_1 Q_1(X/a_n)$ et $n_2 Q_2(X/a_n)$ sont à coefficients dans $\mathbb{Z}$. On a alors exhibé une factorisation de Q en deux polynômes non inversibles, ce qui contredit son irréductibilité. Par l'absurde, $\frac{1}{c(\phi(Q))}\phi(Q)$ est irréductible.

1.3 Se débarrasser des facteurs multiples

On a maintenant un polynôme unitaire. La prochaine chose à faire est de repérer ses facteurs multiples. Si on sait comment factoriser un polynôme sans facteur multiple, et qu'on sait calculer, pour tout polynôme P, le produit Q des facteurs multiples de P avec leur multiplicité décrémentée de 1, alors on saura factoriser P. En effet, on peut alors factoriser P/Q qui est sans facteurs multiples, et, les multiplicités des facteurs de Q étant réduites de 1, on peut appeler récursivement notre algorithme sur Q avec la garantie qu'il se termine.

Théorème Si E est la famille des facteurs irréductibles de $P \in \mathbb{Z}[X]$ (comme défini dans l'introduction), où P est unitaire, alors :

$$pgcd(P, P') = \prod_{\substack{(Q,\, m) \in E \\ m>1}} Q^{m-1}.$$

Preuve Soit donc $D = pgcd(P, P')$. Etant un diviseur de $P = \prod_i Q_i^{m_i}$, et en rappelant que $\mathbb{Z}[X]$ est factoriel, D s'écrit $\prod_i Q_i^{n_i}$, avec pour tout i, $n_i \leqslant m_i$. Fixons-nous un indice i. Il faut montrer $n_i = m_i - 1$. Pour $R = \prod_{j \neq i} Q_j^{m_j}$, on a $P' = (Q_i^{m_i} R)' = m_i Q_i' Q_i^{m_i - 1} R + Q_i^{m_i} R'$. Il apparait bien que $Q_i^{m_i - 1}$ divise P', et donc D. Ainsi, $m_i - 1 \leqslant n_i \leqslant m_i$. Il reste juste à montrer que $Q_i^{m_i}$ ne divise pas D. Pour cela, on se sert du fait que Q_i et R sont premiers entre eux (ainsi que m_i, car Q_i est primitif), et que $P' \equiv m_i Q_i' Q_i^{m_i - 1} R \pmod{Q_i^{m_i}}$. Par l'absurde, si $Q_i^{m_i}$ divise P', alors Q_i divise $Q_i' R$. Comme $\mathbb{Z}[X]$ est factoriel, le

lemme de Gauss affirme que Q_i divise Q_i'. C'est bien sûr faux, car Q_i n'est pas constant, et que le reste de la division euclidienne de Q_i' par Q_i n'est autre que Q_i' (son degré est strictement plus petit), et $Q_i' \neq 0$. Par l'absurde, on a bien que $Q_i^{m_i}$ n'est pas un diviseur de D. Donc $n_i = m_i - 1$, et $D = \prod_{\substack{(Q,\, m)\in E \\ m>1}} Q^{m-1}$.

En divisant P par $pgcd(P, P')$, on se ramène donc a un produit de facteurs irréductibles de multiplicité 1. Bien qu'il est facile de calculer P', calculer le PGCD est moins évident, car l'algorithme d'Euclide ne fonctionne pas dans $\mathbb{Z}[X]$. C'est là que l'on se sert du fait que P est unitaire.

Théorème Soit P un polynôme unitaire de $\mathbb{Z}[X]$. Tous les diviseurs de P dans $\mathbb{Q}[X]$ sont associés dans $\mathbb{Q}[X]$ à un polynôme unitaire de $\mathbb{Z}[X]$.

Preuve Prenons donc P un polynôme unitaire de $\mathbb{Z}[X]$, et Q_1 un diviseur de P dans $\mathbb{Q}[X]$. Sans perte de généralités, on peut supposer Q_1 unitaire (sans être nécessairement à coefficients dans $\mathbb{Z}$) : il suffit de le multiplier par l'inverse (inversible) de son coefficient dominant, qui est alors un polynôme unitaire associé à Q_1. Il faut maintenant montrer que Q_1 est à coefficients dans $\mathbb{Z}$. Soit $Q_2 = P/Q_1$ un polynôme unitaire de $\mathbb{Q}[X]$. Ecrivons $Q_1 = \sum_i \frac{p_i}{q_i} X^i$, où $\frac{p_i}{q_i}$ est l'unique représentant du i-ème coefficient de Q_1 sous forme de fraction irréductible au dénominateur dans $\mathbb{N}^*$. De même, $Q_2 = \sum_i \frac{r_i}{s_i} X^i$. Alors, pour $n_1 = ppcm_i(q_i)$, et $n_2 = ppcm_i(s_i)$, $n_1 Q_1$ et $n_2 Q_2$ sont à coefficients dans $\mathbb{Z}[X]$, et leur produit vaut $n_1 n_2 P$. En examinant les contenus, comme $c(P) = 1$, $c(n_1 n_2 P) = n_1 n_2$. Or, $n_1 Q_1$ et $n_2 Q_2$ sont primitifs. En effet, soit d un diviseur commun de tous les coefficients de $n_1 Q_1$. Si on suppose par l'absurde $d > 1$, alors $\frac{n_1}{d} Q_1 \in \mathbb{Z}[X]$. Donc pour tout i, $\frac{n_1 p_i}{d q_i} \in \mathbb{Z}$, c'est à dire que $m p_i$ est un multiple de q_i, où m est l'entier égal à n_1/d. Comme p_i et q_i sont premiers entre eux, le lemme de Gauss affirme que m est un multiple de q_i. Donc m est un multiple commun de tous les q_i, qui divise strictement n_1 le ppcm de tous les q_i. C'est absurde. Ainsi, $n_1 Q_1$ est primitif, et de même, $n_2 Q_2$ l'est aussi. On en déduit que $c(n_1 Q_1 n_2 Q_2) = 1$, c'est à dire $n_1 n_2 = 1$, c'est à dire $n_1 = 1$ et $n_2 = 1$, c'est à dire $Q_1 \in \mathbb{Z}[X]$ et $Q_2 \in \mathbb{Z}[X]$.

Par conséquent, pour calculer le pgcd dans $\mathbb{Z}[X]$ d'un polynôme unitaire et d'un polynôme quelconque, il suffit de calculer ce pgcd dans $\mathbb{Q}[X]$ (avec l'algorithme d'Euclide), et de le rendre unitaire. Le résultat sera nécessairement dans $\mathbb{Z}[X]$. Etant un pgcd dans $\mathbb{Q}[X]$, c'est aussi un pgcd dans $\mathbb{Z}[X]$.

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

Nous allons donner ici une méthode pour factoriser les polynômes sans facteur multiple de $\mathbb{F}_p[X]$. Nous verrons ensuite comment ramener le problème de factorisation dans $\mathbb{Z}[X]$ à un problème dans $\mathbb{F}_p[X]$. Pour $P \in \mathbb{F}_p[X]$, définissons **une factorisation non triviale** de P comme un couple $(P_1,\ P_2)$ tel que $P = P_1P_2$, et que P_1 et P_2 ne sont associés ni à 1, ni à P. L'algorithme de factorisation de Berlekamp est alors le suivant :

$Berlekamp(P)$:
| Si P est irréductible :
| | return $\{(P,\ 1)\}$
| $(P_1,\ P_2) \leftarrow$ une factorisation non triviale de P
| return $Berlekamp(P_1) \cup Berlekamp(P_2)$
Fin

Sous cette forme, cet algorithme est très simple. Ce qui l'est moins, c'est comment construire les fonctions auxiliaires qui testent si P est irréductible, et, le cas non échéant, lui trouvent une factorisation non triviale. C'est ce que nous allons voir maintenant.

2.1 Test de primalité

Nous allons présenter une méthode pour calculer le nombre de facteur irréductibles d'un polynôme $P \in \mathbb{F}_p[X]$ sans facteur multiple. Si ce nombre est 1, on sait alors que P est irréductible.

Théorème Soit r le nombre de facteurs irréductibles de P. Alors $E_P := \{Q \in \mathbb{F}_p[X]/(P) | Q^p - Q = 0\}$ a p^r éléments. C'est en fait un $\mathbb{F}_p$-espace vectoriel de dimension r.

Preuve Soient $(P_i)_i$ les facteurs irréductibles de P. On doit d'abord utiliser le théorème chinois pour avoir :

$$\mathbb{F}_p[X]/(P) \approx \mathbb{F}_p[X]/(P_1) \times ... \times \mathbb{F}_p[X]/(P_r).$$

Par isomorphisme, on a alors une bijection entre E_P et $E_{P_1} \times ... \times E_{P_r}$. Dans $\mathbb{F}_p[X]/(P_i)$, qui est un corps de caractéristique p (car P_i est irréductible), E_{P_i} est l'ensemble des racines de $X^p - X$, vu dans $(\mathbb{F}_p[X]/(P_i))[X]$. Les p éléments du sous-corps premier de $\mathbb{F}_p[X]/(P_i)$ sont des racines de ce polynôme. Or, il y en a au plus $p = deg(X^p - X)$, et ce sont donc les seules. Le cardinal de E_{P_i} est donc p, et par équipotence, celui de E_P est p^r.

En rappelant que l'endomorphisme de Frobenius $\mathbb{F}_p[X]/(P) \to \mathbb{F}_p[X]/(P)$ est linéaire, E_p est alors un F_p-espace vectoriel en tant que noyau d'une combinaison linéaire d'applications linéaires. Comme son cardinal est p^r, sa dimension est r.

Pour calculer r, on a donc juste besoin de calculer le noyau de la bonne matrice, ce qui se fait facilement avec le pivot de Gauss.

2.2 Section d'un polynôme non irréductible

Soit P un polynôme non irréductible sans facteur multiple de $\mathbb{F}_p[X]$. Comme E_P est un espace vectoriel de dimension au moins 2, il existe une classe $A \in E_P$ tel que A est non constant (le reste de la division euclidienne d'un polynôme de A par P est un polynôme non constant). Soit donc Q le reste de la division euclidienne d'un polynôme de A par P.

Théorème Avec les suppositions ci-dessus, P est associé à $\prod_{n\in\mathbb{F}_p} pgcd(P,\ Q-n)$.

Preuve Pour n et n' dans $\mathbb{F}_p$, $Q-n$ et $Q-n'$ sont étrangers, car $\frac{1}{n'-n}(Q-n)+\frac{1}{n-n'}(Q-n') = 1$. Comme $\mathbb{F}_p[X]$ est principal, ils sont premiers entre eux, et n'ont pas de diviseur commun non inversible. Donc aucun facteur de $\prod_{n\in\mathbb{F}_p} pgcd(P,\ Q-n)$ n'apparait plusieurs fois, et ce produit divise bien P. Réciproquement soit $\phi : \mathbb{F}_p[X] \to \mathbb{F}_p[X]$ l'endomorphisme d'évaluation induit par la restriction canonique $\mathbb{F}_p \to \mathbb{F}_p[X]$, et par l'élément du codomaine Q (c'est à dire $\phi(R) = R(Q)$, pour tout polynôme R). Comme la classe de Q est dans E_P, on sait que $\phi(X^p - X) = Q^p - Q \equiv 0 \pmod{P}$. Or, on sait aussi que $X^p - X$ est scindé dans $\mathbb{F}_p[X]$, et que ses p racines sont les éléments du sous-corps premier de $\mathbb{F}_p[X]$.

$$\begin{aligned}\text{Donc } \phi(X^p - X) &= \phi\left(\prod_{n\in\mathbb{F}_p} X - n\right)\\ &= \prod_{n\in\mathbb{F}_p} \phi(X-n)\\ &= \prod_{n\in\mathbb{F}_p} Q - n.\end{aligned}$$

Donc P divise bien $\prod_{n\in\mathbb{F}_p} Q-n$. Le théorème est démontré.

Sachant que le degré de Q est strictement plus petit que celui de P, un des facteurs de $\prod_{n\in\mathbb{F}_p} Q-n$ va alors être un diviseur non trivial de P, qui fournit directement la factorisation non triviale $(P,\ P/Q)$. Dans $\mathbb{F}_p[X]$, un PGCD se calcule facilement avec l'algorithme d'Euclide.

Ainsi, on sait comment factoriser n'importe quel polynôme sans facteur multiple de $\mathbb{F}_p[X]$.

3 De $\mathbb{F}_p[X]$ à $\mathbb{Z}[X]$

Quels sont les liens entre la factorisation d'un polynôme P dans $\mathbb{Z}[X]$, et sa factorisation dans $\mathbb{F}_p[X]$? Passer de l'un à l'autre n'a rien de trivial, mais nous allons voir comment faire.

3.1 Majorer les coefficients des facteurs

Définitions On va définir les normes usuelles d'un polynôme. Soit $P = \sum_{n\in\mathbb{N}} a_n X^n \in \mathbb{Z}[X]$. Pour $\lambda \leqslant 1$, nous noterons $||P||_\lambda = \left(\sum_{n\in\mathbb{N}} |a_n|^\lambda\right)^{\frac{1}{\lambda}}$, et $||P||_\infty = max_{n\in\mathbb{N}}|a_n|$.

Remarque Si λ et μ sont dans $[1,\ +\infty]$ tels que $\lambda \leqslant \mu$, on a alors $||P||_\mu \leqslant ||P||_\lambda$.

Supposons que, pour Q un facteur irréductible du polynôme à factoriser P, on ait trouvé un $M \in \mathbb{N}$ tel que $||Q||_\infty < 2M$. Alors, si on connaît les coefficients de Q modulo $2M$, on connait leur valeur exacte : leur unique représentant dans $[-M,\ M]$.

Nous allons donc montrer comment trouver une telle majoration.

Théorème Soit P dans $\mathbb{Z}[X]$. Pour tout Q diviseur de P, on a $||Q||_1 \leqslant 2^{degP}||P||_2$, et $||Q||_\infty \leqslant \binom{degP}{\frac{1}{2}degP}||P||_2$.

Preuve La preuve fait appel à des résultats d'analyse complexe que nous admettrons.

On définit la mesure d'un polynôme R comme $M(R) = |a_R|\prod_i max(1,\ |\alpha_{i,R}|)$, où a_R est le coefficient dominant de R, et $(\alpha_{i,R})_i$ sont les racines complexes (non nécessairement distinctes) de R. Si $R \in \mathbb{Z}[X]$, $|a_R| \geqslant 1$, et donc $M(R) \geqslant 1$. De plus, M est multiplicative, c'est à dire $M(RS) = M(R)M(S)$.

Tout d'abord, pour a_k le coefficient de degré k de Q, on a $|a_k| \leqslant \binom{degQ}{k}M(Q)$ (admis). On a alors par somme $||Q||_1 \leqslant 2^{degQ}M(Q)$, et comme $max_k\binom{degQ}{k} = \binom{degQ}{\frac{1}{2}degQ}$, on a $||Q||_\infty \leqslant \binom{degQ}{\frac{1}{2}degQ}M(Q)$. Sachant que Q divise P, on a alors $degQ \leqslant degP$ et $M(Q) \leqslant M(Q)M(P/Q) = M(P)$.

Donc $||Q||_1 \leqslant 2^{degP}M(P)$ et $||Q||_\infty \leqslant \binom{degP}{\frac{1}{2}degP}M(P)$.

On a de plus $M(P) \leqslant ||P||_2$ (admis). Avec les deux inégalités ci dessus, le théorème est alors clair.

Remarque Si P n'est pas irréductible, l'un de ses facteurs irréductibles a un degré au plus égal à $\frac{1}{2}degP$. On peut donc baisser notre borne à $\binom{\frac{1}{2}degP}{\frac{1}{4}degP}||P||_2$.

3.2 Recombiner les facteurs

Soit P, dont la factorisation complète dans $\mathbb{Z}[X]$ est $\prod_{i\in I} P_i$ sans facteur multiple. Soit $\prod_{j\in J} Q_j$ sa factorisation complète dans $\mathbb{F}_p[X]$, qu'on supposera aussi sans facteur multiple. On peut commencer par remarquer le fait suivant :

Propriété Soit $\phi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ la surjection canonique (en identifiant $\mathbb{F}_p$ à $\mathbb{Z}/(p)$). Avec les suppositions ci-dessus, on a que pour tout j dans J, il existe un unique i dans I tel que Q_j divise $\phi(P_i)$.

Preuve La preuve est très simple. Pour chaque i dans I, soit $\prod_{k\in K_i} R_{k,i}$ la factorisation complète de $\phi(P_i)$ dans $\mathbb{F}_p[X]$. On a alors $\prod_{j\in J} Q_j = \prod_{i\in I}\prod_{k\in K_i} R_{k,i}$. Comme $\mathbb{F}_p[X]$ est factoriel, pour tout j dans J, il existe un i dans I et un k dans K_i tels que Q_j et $R_{k,i}$ sont associés, c'est à dire que Q_j divise $\phi(P_i)$. De plus, ce i est unique, car il n'y a pas de facteurs multiples : si $R_{k,i}$ est associé à $R_{k',i'}$, on a $(k,\ i) = (k',\ i')$.

Cette propriété nous dit en fait qu'une factorisation dans $\mathbb{F}_p[X]$ sera toujours plus "fine" qu'une factorisation dans $\mathbb{Z}[X]$. Métaphoriquement, si P est un gâteau, et sa factorisation dans $\mathbb{Z}[X]$ un certain découpage du gâteau, alors factoriser P dans $\mathbb{F}_p[X]$ revient à reprendre ce découpage, et éventuellement d'y ajouter des coups de couteau supplémentaires. Quand on lit la preuve ci-dessus, la propriété paraît élémentaire, mais elle permet en fait d'énoncer le corollaire suivant :

Corollaire Avec les mêmes suppositions, pour tout i dans I, il existe une partie $E_i \subset J$ telle que $\phi(P_i) = \prod_{j\in E_i} Q_j$.

Preuve On construit $E_i = \{j \in J | Q_j \text{ divise } \phi(P_i)\}$, qui vérifie bien le corollaire.

Ainsi, si on factorise p dans $\mathbb{F}_p[X]$, avec p plus grand que la borne de la partie précédente, il suffit de prendre tous les sous-produits possibles de notre factorisation, de choisir les représentants de leurs coefficients dans $[-p/2,\ p/2]$, et de vérifier si l'un des sous-produits est un diviseur non trivial de P. Si aucun ne

l'est, P est nécessairement irréductible. Sinon, on aura "recombiné" le diviseur trouvé.

Remarques

— Ci-dessus, on voit tout de suite apparaître un algorithme de factorisation pour $\mathbb{Z}[X]$. Une optimisation va néanmoins être présentée dans la partie suivante, pour éviter de travailler dans un corps trop grand.

— Le "découpage" dans un corps fini peut être **strictement** plus fin que dans $\mathbb{Z}$. Un exemple connu est le polynôme X^4+1, qui est irréductible sur $\mathbb{Z}$, et réductible dans tout corps premier fini. Le fait de devoir recombiner les facteurs en examinant toutes les parties de J est donc absolument nécessaire.

3.3 La remontée de Hensel

Quand on recherche un nombre premier plus grand que la borne présentée précédemment, l'apparition de coefficients binomiaux fait grimacer, car leur comportement asymptotique fait intervenir l'exponentielle.

La remontée de Hensel donne une bonne optimisation, qui permet de déduire, d'une factorisation de P dans $\mathbb{F}_p$ avec p quelconque (on le veut petit), une factorisation de P dans $\left(\mathbb{Z}/p^k\mathbb{Z}\right)[X]$, où k est aussi grand que l'on veut (et on le veut tel que $p^k \geqslant 2\binom{\frac{1}{2}degP}{\frac{1}{4}degP}||P||_2$).

Définition Pour A et B deux polynômes tels que B est unitaire, on notera $Div(A,\ B)$ le couple $(Q,\ R)$ tel que Q est le quotient et R le reste de la division euclidienne de A par B.

Données de départ Soit $m \leqslant 2$, $A = \mathbb{Z}/m\mathbb{Z}$ et $A' = \mathbb{Z}/m^2\mathbb{Z}$. Notons $\phi : \mathbb{Z}[X] \to A[X]$ et $\psi : \mathbb{Z}[X] \to A'[X]$ les surjections canoniques. Remarquons que, si $\phi(P_1) = \phi(P_2) = 0$, alors $\psi(P_1P_2) = 0$. Soit P dans $\mathbb{Z}[X]$ le polynôme (unitaire, et sans facteur multiple) que l'on souhaite factoriser. Nous avons au départ quatre polynômes B, C, U et V dans $\mathbb{Z}[X]$ tels que :

— $degB + degC = degP$.

— $\phi(BC) = \phi(P)$.

— C est unitaire.

— $\phi(BU + CV) = 1$.

— $degU < degC$ et $degV < degB$.

Objectif A partir de ces quatre polynômes, nous souhaitons construire quatre nouveaux polynômes B_2, C_2, U_2 et V_2 tels que :

— $\phi(B) = \phi(B_2),\ \phi(C) = \phi(C_2),\ \phi(U) = \phi(U_2),\ \phi(V) = \phi(V_2)$.

— $degB_2 + degC_2 = degP$.

— $\psi(B_2C_2) = \psi(P)$.

— C_2 est unitaire.
— $\psi(B_2U_2 + C_2V_2) = 1$.
— $degU_2 < degC_2$ et $degV_2 < degB_2$.

Soit $\psi_2 : A'[X] \to \mathbb{Z}$ qui associe à chaque classe son unique représentant dont les coefficients ont une valeur positive strictement plus petite que m^2 (le reste de la division euclidienne par m^2). On remarque que $\phi \circ \psi_2 \circ \psi = \phi$ (car $m^2\mathbb{Z}[X] \subset m\mathbb{Z}[X]$), et $\psi \circ \psi_2 = Id$. Soit $(Q,\ R) = Div(U(P - BC),\ C)$.

Montrons déjà que $\phi(Q) = 0 = \phi(R)$. Sachant que $P - BC \in m\mathbb{Z}[X]$, soit $(Q_0,\ R_0) = Div(\frac{1}{m}U(P - BC),\ C)$. On a alors $m(\frac{1}{m}U(P - BC)) = m(Q_0C + R_0) = (mQ_0)C + mR_0$, avec $degmR_0 < degC$. La division euclidienne étant unique, on a alors $(Q,\ R) = (mQ_0,\ mR_0)$, et ainsi $\phi(Q) = 0 = \phi(R)$.

Construction de B_2 et C_2 Nous construisons alors $B_2 = (\psi_2 \circ \psi)(B + V(P - BC) + QB)$, et $C_2 = C + R = C + U(P - BC) - QC$. Comme $\phi(P - BC) = \phi(Q) = \phi(R) = 0$, on a bien $\underline{\phi(B_2) = \phi(B)}$ et $\underline{\phi(C_2) = \phi(C)}$. Comme $degR < degC$, $\underline{C_2 \text{ est bien unitaire}}$, et $\underline{degC_2 = degC}$. De plus :

$$\begin{aligned}
\psi(P - B_2C_2) &= \psi(P - (B + V(P - BC) + QB)(C + U(P - BC) - QC)) \\
&= \psi(P - BC - UV(P - BC)^2 - (BU + CV)(P - BC) \\
&\qquad + Q^2BC + Q(P - BC)(CV + BU)) \\
&= \psi(-UV(P - BC)^2 - (BU + CV - 1)(P - BC) \\
&\qquad + Q^2BC + Q(P - BC)(CV + BU))
\end{aligned}$$

Or nous avons :
— $\psi((P - BC)^2) = 0$
— $\psi((BU + CV - 1)(P - BC)) = 0$
— $\psi(Q^2) = 0$
— $\psi(Q(P - BC)) = 0$

Donc $\underline{\psi(P - B_2C_2) = 0}$. Comme le coefficient dominant de B_2 n'est pas un multiple de m^2 (car $B_2 \in Im(\psi_2)$), et que C_2 est unitaire, le coefficient dominant de B_2C_2 n'est pas un multiple de m^2. Il en est de même pour P qui est unitaire. Comme le coefficient dominant de $P - B_2C_2$ est un multiple de m^2, nous avons nécessairement $\underline{degB_2 + degC_2 = degP}$.

On a bien vérifié que B_2 et C_2 possédaient toutes les propriétés attendues. Il faut maintenant construire U_2 et V_2.

Soit $(Q_2,\ R_2) = Div(U(UB_2 + VC_2 - 1),\ C_2)$. Sachant que $\phi(UB_2 + VC_2 - 1) = 0$, avec le même argument que pour Q et R, nous avons $\phi(Q_2) = 0 = \phi(R_2)$.

Construction de U_2 et V_2 Nous construisons alors $U_2 = (\psi_2 \circ \psi)(U - R_2) = (\psi_2 \circ \psi)(U - U(UB_2 + VC_2 - 1) + Q_2C_2)$, et $V_2 = (\psi_2 \circ \psi)(V(2 - UB_2 - VC_2) - Q_2B_2)$.

Comme $degR_2 < degC_2$ et $degU < degC = degC_2$, nous avons bien $\underline{degU_2 < degC_2}$. Comme $\phi(R_2) = 0$, nous avons bien $\underline{\phi(U_2) = \phi(U)}$. De même, comme $\phi(1 - UB_2 + VC_2) = 0 = \phi(Q_2)$, nous avons $\underline{\phi(V_2) = \phi(V)}$. On a aussi :

$$\begin{aligned}\psi(U_2B_2 + V_2C_2 - 1) &= \psi((U - U(UB_2 + VC_2 - 1) + Q_2C_2)B_2 \\ &\quad +(V(2 - UB_2 - VC_2) - Q_2B_2)C_2 - 1) \\ &= \psi(UB_2 + VC_2 - (UB_2 + VC_2)(UB_2 + VC_2 - 1) - 1) \\ &= \psi(-(UB_2 + VC_2 - 1)^2) \\ &= \underline{0}\end{aligned}$$

Pour finir, en supposant que B, C et P sont non constants, le coefficient de $U_2B_2 + V_2C_2 - 1$ est un multiple de m^2, tandis que ceux de U_2, V_2 et B_2 ne sont pas des multiples de m^2. Comme C_2 est unitaire, le coefficient dominant de V_2C_2 n'est pas non plus un multiple de m^2 (peut être que celui de U_2B_2 en est un). On en déduit $degU_2 + degB_2 \geqslant degV_2 + degC_2$. En sommant avec l'inégalité $-degU_2 > -degC_2$, nous obtenons $\underline{degB_2 > degV_2}$.

Nous avons bien construit B_2, C_2, U_2 et V_2 pour qu'ils satisfassent les propriétés attendues.

Cette méthode nous permet de passer d'une factorisation (complète) de P dans $\mathbb{F}_p[X]$ à une factorisation (quelconque) dans $(\mathbb{Z}/(p^k))[X]$. La borne est dépassée avec un nombre d'itérations logarithmique. Comme la factorisation de départ est complète, le raisonnement sur la recombinaison des facteurs fonctionne avec la factorisation d'arrivée.

Remarques

- Il est indispensable que C et C_2 soient unitaires, sinon la division euclidienne n'existe pas toujours.
- Si les conditions sur les degrés ne sont pas respectées, on produit des facteurs avec un degré trop grand et la recombinaison ne fonctionnera pas.
- A l'initialisation (dans $\mathbb{F}_p[X]$), il ne faut pas oublier de rendre C unitaire en le multipliant par l'inverse de son coefficient dominant. Il ne faut pas utiliser l'algorithme d'Euclide-Bézout pour calculer la relation de Bézout, car les polynômes U et V produits auront peut-être des degrés trop grands. Il faut plutôt résoudre un système linéaire dont les inconnues sont les coefficients de U et V.

4 Implémentation

4.1 En résumé

Le programme consiste surtout à manipuler des tableaux Java. Les systèmes linéaires sont résolus avec le pivot de Gauss, les pgcd calculés avec l'algorithme d'Euclide. Les inverses dans $\mathbb{F}_p$ sont calculés avec l'algorithme d'Euclide-Bézout.

4.2 Trouver le bon nombre premier

Pour factoriser P sur un corps, il faut trouver un nombre premier p tel que P est sans facteur multiple dans $\mathbb{F}_p[X]$. Par exemple, le polynôme $X^2 - 3$, qui est irréductible dans $\mathbb{Z}[X]$, est le carré $X * X$ dans $\mathbb{F}_3[X]$, et on aura des soucis si on choisit $p = 3$.

Pour bien choisir, une condition suffisante pour qu'un nombre premier p ne pose pas de problèmes est donnée par la propriété suivante (qu'on admettra) :

Propriété Si P a un facteur irréductible de multiplicité plus grande que 1 dans $\mathbb{F}_p[X]$, alors p divise le résultant de P et P' (dans $\mathbb{Z}[X]$).

Le résultant de deux polynômes est le déterminant d'une certaine matrice qui dépend de leurs coefficients. On a donc juste à le calculer, et à choisir un nombre premier qui ne le divise pas.

4.3 Les problèmes d'espace

Dans la formule de la section 1 pour passer d'un polynôme primitif à unitaire, le coefficient dominant est mis à une puissance assez élevée, et les valeurs absolues des coefficients du polynôme unitaire produit peuvent potentiellement exploser. Par exemple, le polynôme $16X^9 + 1$ sera transformé en $X^9 + 2^{32}$. Nous travaillerons ensuite modulo un nombre plus grand que la norme euclidienne de ce polynôme...

Ainsi, les entiers sur 32 bits (ou même 64) ne feront pas l'affaire. Les coefficients des polynômes manipulés seront en fait des objets de la classe *math.BigInteger*, qui permet d'avoir des entiers non bornés.

C'est la même idée pour le calcul d'un discriminant dans $\mathbb{Q}$. Nous avons implémenté les rationnels, et même en les réduisant autant que possible, c'est facile de dépasser la taille d'un entier.

4.4 Les problèmes de temps

La recombinaison des facteurs de P va brutalement examiner les $2^n - 2$ facteurs non triviaux potentiels, où n est le nombre de facteurs irréductibles de P dans $\mathbb{F}_p[X]$. Théoriquement, c'est très inefficace (le pire cas étant atteint quand P est scindé dans $\mathbb{F}_p[X]$, et irréductible dans $\mathbb{Z}[X]$). En pratique, n est souvent petit par rapport au degré de P et le parcours a de bonnes chances de s'arrêter avant d'avoir tout essayé.