Algorithmes pour l'arithmétique II
Cours 5

Julien Lavauzelle

Université Paris 8

Master 2 ACC et CSSD – Algorithmes pour l'arithmétique

05/01/2020

Motivation

Lors de la séance précédente :

Factorisation de polynômes sur les corps finis.

Aujourd'hui :

Factorisation de polynômes sur les rationnels et les entiers.

Références utiles :

[LN] *Introduction to Finite Fields and their Applications, 2nd ed.*. Lidl, Niederreiter. Cambridge University Press. **1994**.

[AECF] *Algorithmes Efficaces en Calcul Formel*. Bostan, Chyzak, Giusti, Lebreton, Lecerf, Salvy, Schost. auto-édition, disponible en ligne sur `https://hal.archives-ouvertes.fr/AECF`. **2017**.

[GG] *Modern Computer Algebra, 3rd ed.*. Gathen, Gerhard. Cambridge University Press. **2003**.

Plan

1. Quelques rappels

2. Factorisation dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$
   Définition du problème
   Élimination des facteurs carrés
   Réduction à la factorisation dans $\mathbb{F}_p[X]$
   Amélioration : lemme de Hensel
   Dernière étape : regroupement des facteurs

3. Exercices

Stratégies de factorisation dans $\mathbb{F}_p[X]$

Soit $P(X) = P_1(X)^{m_1} \dots P_k(X)^{m_k} \in \mathbb{F}_p[X]$ à factoriser.

- Élimination des facteurs carrés :

$$P(X) \quad \to \quad P_1(X) \cdots P_k(X) = P^*(X)\,.$$

- Factorisation sans carré

$$P^*(X) = P_1(X) \cdots P_k(X) \quad \to \quad (P_1(X), \dots, P_k(X))\,.$$

- Factorisation en produit de même degré

$$P^*(X) \quad \to \quad (Q_1(X), \dots, Q_r(X)) \quad \text{où } Q_d = \prod_{j \mid \deg P_j = d} P_j(X)\,.$$

- Factorisation à degré égal

$$Q_d(X) \quad \to \quad \big(P_j(X)\big)_{j \mid \deg P_j = d}$$

Algorithme de Berlekamp en petite cardinalité

Entrée : un polynôme $P = \prod_{i=1}^{k} P_i$ sans facteur carré
Sortie : un diviseur propre Q de P

1. Calculer la matrice $\boldsymbol{M}$ de ϕ dans la base polynomiale $(1, \alpha, \ldots, \alpha^{n-1})$.
2. Calculer un élément $(b_0 = 0, \ldots, b_{n-1})$ du noyau de $\boldsymbol{M}$ tel que $b_j \neq 0$ pour au moins un $j \geq 1$.
3. Construire $B(X) = \sum_{j=0}^{n-1} b_j X^j$
4. **Faire :**
   - Choisir un nouveau $\lambda \in \mathbb{F}_q$ — déterministe (énumération) ou probabiliste.
   - Calculer $Q(X) = \mathrm{pgcd}(P(X), B(X) - \lambda)$.

   tant que $Q(X) = 1$.
5. Retourner Q.

ALGORITHME DE FACTORISATION EN DEGRÉ DISTINCTS

Entrée : $P \in \mathbb{F}_q[X]$
Sortie : la factorisation $P = Q_1 Q_2 \dots Q_s$ où Q_r est le produit de tous les diviseurs de P irréductibles et de degré r

1. Poser $Q \leftarrow P$, $S \leftarrow X$, et $i \leftarrow 1$
2. **Tant que** $Q \neq 1$
   - 2.1 Calculer $S \leftarrow S^q \mod P$
   - 2.2 Calculer $Q_i \leftarrow \mathrm{pgcd}(Q, S - X)$
   - 2.3 Calculer $Q \leftarrow Q/Q_i$
   - 2.4 Incrémenter i
3. Retourner $Q_1, \dots, Q_{i-1}$.

ALGORITHME DE CANTOR-ZASSENHAUS : FACTORISATION À DEGRÉ ÉGAL

Entrée : $Q \in \mathbb{F}_q[X]$ un polynôme de degré $n = sr$, formé de s polynômes irréductibles $P_1, \ldots, P_s$, distincts de degré r
Sortie : des diviseurs propres de Q

1. **Faire :**
   1.1 Tirer uniformément $A(X)$ un polynôme non-nul de degré $\leq n-1$.
   1.2 Calculer $D_0 = \mathrm{pgcd}(A, Q)$.
   1.3 Calculer $S = A^{(q^r-1)/2} \bmod Q$.
   1.4 Calculer $D_1 = \mathrm{pgcd}(A-1, Q)$.

   tant que D_0 ou D_1 n'est pas un diviseur propre de Q.
2. Retourner les diviseurs propres obtenus parmi Q/D_0, D_0, Q/D_1, D_1

Plan

1. Quelques rappels

2. Factorisation dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$
   Définition du problème
   Élimination des facteurs carrés
   Réduction à la factorisation dans $\mathbb{F}_p[X]$
   Amélioration : lemme de Hensel
   Dernière étape : regroupement des facteurs

3. Exercices

Plan

1. Quelques rappels

2. Factorisation dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$
   Définition du problème
   Élimination des facteurs carrés
   Réduction à la factorisation dans $\mathbb{F}_p[X]$
   Amélioration : lemme de Hensel
   Dernière étape : regroupement des facteurs

3. Exercices

Notre objectif

Objectifs. Factoriser dans $\mathbb{Q}[X]$ et/ou dans $\mathbb{Z}[X]$.

Rappel. Factorisation = décomposition en irréductibles, à une unité près.

Exemple. Pour $f = 60X^2 + 10X - 10$:

- Les décompositions $10(2X+1)(3X-1)$ et $60(X+\frac{1}{2})(X-\frac{1}{3})$ sont des factorisations dans $\mathbb{Q}[X]$.
- Ce ne sont pas des factorisations dans $\mathbb{Z}[X]$.
- La décomposition $2 \cdot 5 \cdot (2X+1) \cdot (3X-1)$ en est une.

Définitions, lemme de Gauss

Soit A un anneau factoriel (ex : $A = \mathbb{Z}$) et K son corps des fractions (ex : $K = \mathbb{Q}$).

Définitions. Soit $f = \sum_i f_i X^i \in A[X]$.

- Le **contenu** $\mathrm{cont}(f) \in A$ est le pgcd des coefficients de f.
- Le polynôme f est **primitif** si $\mathrm{cont}(f) = 1$. La partie primitive de f est $f/\mathrm{cont}(f)$.
- Le **coefficient de tête** est $\mathrm{lc}(f)$ et, si $f \in \mathbb{Z}[X]$, $\|f\|_\infty = \max\{|f_i|\}$

Exemple. Si $f = 6X^2 + 15$:

- son contenu est $\mathrm{cont}(f) = 3$
- et sa partie primitive est $f^* = 2X^2 + 5$.

Lemme (de Gauss). Soit $f \in A[X]$. Alors, f est irréductible dans $A[X]$ si et seulement si f est primitif et f est irréductible dans $K[X]$.

Corollaire. L'anneau $A[X]$ est aussi factoriel. Les irréductibles de $A[X]$ sont

1. les irréductibles de A,
2. les éléments de $A[X]$, irréductibles dans $K[X]$ et primitifs.

Exemple : le polynôme $f = 6X^2 + 15$ est irréductible dans $\mathbb{Q}[X]$ mais pas dans $\mathbb{Z}[X]$.

Réduction des factorisations dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$

Objectifs. Factoriser dans $\mathbb{Q}[X]$ et/ou dans $\mathbb{Z}[X]$.

Question. Deux problèmes calculatoirement équivalents ?

Exemple 1. Si $f = 60X^2 + 10X - 10$.

- La factorisation $2 \cdot 5 \cdot (2X+1) \cdot (3X-1)$ dans $\mathbb{Z}[X]$ donne aussi une factorisation dans $\mathbb{Q}[X]$ (on peut multiplier les termes constants).
- Même à partir de $60(X+\frac{1}{2})(X-\frac{1}{3}) \in \mathbb{Q}[X]$, on peut obtenir une factorisation dans $\mathbb{Z}[X]$ en multipliant/divisant par le ppcm des dénominateurs :

$$60(X+\tfrac{1}{2})(X-\tfrac{1}{3}) \;\rightarrow\; 10(2X+1)(3X-1) \rightarrow 2 \cdot 5 \cdot (2X+1) \cdot (3X-1)$$

Exemple 2. Si $g = 24178516392919305121959 89X + 24178516392919305121959 89$.

- Dans $\mathbb{Q}[X]$, on peut obtenir la factorisation $24178516392919305121959 89(X+1)$.
- Pour obtenir une factorisation dans $\mathbb{Z}[X]$, il faut également factoriser le contenu :

$$24178516392919305121959 89 = 1099511627791 \times 2199023255579$$

ce qui n'est pas immédiat.

Réduction des factorisations dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$

- $(\mathbb{Z}[X] \implies \mathbb{Q}[X] + \mathbb{Z})$ Une factorisation dans $\mathbb{Z}[X]$

$$f = \alpha_1 \cdots \alpha_r f_1 \cdots f_s,$$

où $\alpha_i \in \mathbb{Z}$ est irréductible dans $\mathbb{Z}$ et $f_j \in \mathbb{Z}[X]$ est primitif et irréductible dans $\mathbb{Q}[X]$, donne immédiatement
  - une factorisation de f dans $\mathbb{Q}[X]$ (le produit $\alpha_1 \cdots \alpha_r$ étant une unité dans $\mathbb{Q}[X]$)
  - ainsi qu'une factorisation du contenu $\mathrm{cont}(f) = \alpha_1 \cdots \alpha_r \in \mathbb{Z}$.

- $(\mathbb{Q}[X] + \mathbb{Z} \implies \mathbb{Z}[X])$ Réciproquement, si

$$f = f_1^* \cdots f_s^* \quad \text{et} \quad \mathrm{cont}(f) = \alpha_1 \cdots \alpha_r$$

sont des factorisations de f dans $\mathbb{Q}[X]$ et de $\mathrm{cont}(f)$ dans $\mathbb{Z}$, alors on peut calculer

$$\lambda_j = \mathrm{ppcm}\{ \text{ dénominateurs des coefficients de } f_j^* \ \}.$$

On a ensuite

$$\lambda_j f_j^* = \mathrm{cont}(\lambda_j f_j^*) f_j \ \in \mathbb{Z}[X]$$

où $f_j \in \mathbb{Z}[X]$ est primitif et irréductible dans $\mathbb{Q}[X]$. Puis,

$$f = f_1^* \cdots f_s^* = \underbrace{\left(\frac{1}{\lambda_1 \cdots \lambda_s} \cdot \mathrm{cont}(\lambda_1 f_1^*) \cdots \mathrm{cont}(\lambda_s f_s^*) \right)}_{= \frac{\mathrm{cont}(\lambda_1 \cdots \lambda_s f_1^* \cdots f_s^*)}{\lambda_1 \cdots \lambda_s} = \mathrm{cont}(f) = \alpha_1 \cdots \alpha_r} f_1 \cdots f_s$$

Réduction des factorisations dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$

Conséquence.

$$\text{factoriser dans } \mathbb{Z}[X] \iff \text{factoriser dans } \mathbb{Q}[X] + \text{factoriser dans } \mathbb{Z}$$

Il s'avère que :

1. On ne connaît pas d'algorithme polynomial pour factoriser dans $\mathbb{Z}$, même si certains sont sous-exponentiels (cf. cours suivants).
2. Il existe un algorithme polynomial (qu'on va aborder dans ce cours) pour factoriser des polynômes de $\mathbb{Q}[X]$, ou encore des polynômes **primitifs** de $\mathbb{Z}[X]$.

Nouvel objectif. Étant donné $f \in \mathbb{Z}[X]$ **primitif**, factoriser f.

Stratégie

Stratégie de factorisation lorsque $f \in \mathbb{Z}[X]$ est primitif.

1. On **élimine les facteurs carrés** dans f, en calculant $\mathrm{pgcd}(f, f')$.
2. On **choisit un « grand » nombre premier** p, respectant certaines conditions de divisibilité.
3. On calcule $g = f \bmod p$, puis une **factorisation de** g **dans** $\mathbb{F}_p[X]$.
4. On **regroupe les facteurs** obtenus pour obtenir la factorisation dans $\mathbb{Z}[X]$.

Plan

1. Quelques rappels

2. Factorisation dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$
   - Définition du problème
   - Élimination des facteurs carrés
   - Réduction à la factorisation dans $\mathbb{F}_p[X]$
   - Amélioration : lemme de Hensel
   - Dernière étape : regroupement des facteurs

3. Exercices

Première étape

1. On **élimine les facteurs carrés** dans f, en calculant $\mathrm{pgcd}(f, f')$.

C'est identique au cas des corps finis, et **sans le problème de la « séparabilité »**.

Si $f = f_1^{m_1} \cdots f_s^{m_s}$, alors

$$f' = \sum_{i=1}^{s} m_i f_i' \frac{f}{f_i}.$$

Puis,

$$\mathrm{pgcd}(f, f') = f_1^{m_1 - 1} \cdots f_s^{m_s - 1}$$

et

$$\frac{f}{\mathrm{pgcd}(f, f')} = f_1 \cdots f_s$$

est la partie sans carré de f.

Complexité. On peut faire les opérations dans $\mathbb{Z}$ ou dans $\mathbb{Q}$. On doit effectuer un nombre logarithmique $O^{\sim}(\deg f)$ d'opérations dans $\mathbb{Z}$ ou $\mathbb{Q}$.

rappel : $O^{\sim}(u) = \cup_d O(u \log^d u)$

Remarque. La taille des coefficients peut grossir exponentiellement. Certaines techniques pour résoudre ce problème (pgcd modulaire par exemple).

Plan

1. Quelques rappels

2. Factorisation dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$
   - Définition du problème
   - Élimination des facteurs carrés
   - Réduction à la factorisation dans $\mathbb{F}_p[X]$
   - Amélioration : lemme de Hensel
   - Dernière étape : regroupement des facteurs

3. Exercices

Suite de l'algorithme

2. On **choisit un « grand » nombre premier** p, respectant certaines conditions de divisibilité.
3. On calcule $g = f \bmod p$, puis une **factorisation de** g **dans** $\mathbb{F}_p[X]$.
4. On **regroupe les facteurs** obtenus pour obtenir la factorisation dans $\mathbb{Z}[X]$.

Question (1). Pourquoi 4. mentionne un regroupement de facteurs ?

Question (2). Quel nombre premier p choisir ?

Concernant la **taille** de p :

- Si p est grand, l'algorithme de factorisation dans $\mathbb{F}_p[X]$ va être coûteux ;
- si p est petit, réussit-on à retrouver le bon résultat ?

Concernant la **forme** de p : tous les p donnent-ils la même (bonne) factorisation ?

Nécessité du regroupement de facteurs

Question (1). Pourquoi **4.** mentionne un regroupement de facteurs ?

Reformulation. Si $f = f_1 \dots f_k \in \mathbb{Z}[X]$, la factorisation de $(f \mod p)$ dans $\mathbb{F}_p[X]$ est-elle

$$(f_1 \mod p) \times \cdots \times (f_k \mod p) \text{ ?}$$

Soit $f \in \mathbb{Z}[X]$ irréductible.

1. Le polynôme f reste-t-il irréductible dans tout $\mathbb{F}_p[X]$?
   Non. Contre-exemple ? $f = X^2 + 1$.
   Pour $p = 2$. Aussi pour tout $p \equiv 1 \mod 4$, car il existe des racines carrées de -1 : l'élément $\omega^{\frac{p-1}{4}}$ où ω est primitif dans $\mathbb{F}_p$, et son opposé.

2. Existe-t-il toujours p tel que le polynôme f est irréductible dans $\mathbb{F}_p[X]$?
   Non. Contre-exemple ? $f = X^4 + 1$.

Exercice. Soit $f = X^4 + 1$. Pour tout premier p, le polynôme f admet un facteur propre dans $\mathbb{F}_p[X]$.

Nécessité du regroupement de facteurs

Exercice. Soit $f = X^4 + 1$. Pour tout premier p, le polynôme f admet un facteur propre dans $\mathbb{F}_p[X]$.

Solution. Pour $p = 2$ c'est clair : $X^4 + 1 = (X+1)^4$.
Sinon... idée : on raisonne « comme dans $\mathbb{C}$ » : on cherche à factoriser f dans $\mathbb{F}_{p^2}[X]$.

Question : f admet-il une racine dans $\mathbb{F}_{p^2}$? **Oui.** Comme p est impair, $p^2 - 1$ est divisible par 8, donc il existe un élément α d'ordre 8 dans $\mathbb{F}_{p^2}^\times$. Autrement dit, α est une racine 4-ème de -1, donc $X - \alpha$ divise f dans $\mathbb{F}_{p^2}[X]$.

La racine α admet un élément conjugué $X - \overline{\alpha}$, et ici $\overline{\alpha} = \alpha^p$. De plus, $X - \overline{\alpha}$ divise aussi f car $\overline{\alpha}^4 = \alpha^{4p} = (-1)^p = -1$.
On a alors

$$(X-\alpha)(X-\alpha^p) = X^2 - \underbrace{(\alpha+\alpha^p)}_{\mathrm{Tr}(\alpha)\in\mathbb{F}_p} X + \underbrace{\alpha^{p+1}}_{\mathrm{N}(\alpha)\in\mathbb{F}_p} \in \mathbb{F}_p[X]$$

qui divise f dans $\mathbb{F}_p[X]$.

Conséquence. L'étape **4.** de regroupement de facteurs obtenus dans $\mathbb{F}_p[X]$ est nécessaire (dans le pire cas).

Quelle taille pour p ? Exemples.

Question (2). Quel nombre premier p choisir ?

Exemple : $f = X^3 - 6X^2 + 11X - 6$.

- Si l'on essaie avec $p \leq 11$, les coefficients de f modulo p changent, ce qui complique les choses pour retrouver la factorisation de f...
- On essaie avec $p = 13$.
  - Dans $\mathbb{F}_p[X]$, l'algorithme de factorisation retourne les facteurs propres
  $$X - 1 \mod 13, \quad X - 2 \mod 13, \quad X - 3 \mod 13\,.$$
  - On a bien $(X-1)(X-2)(X-3) = f$
- Mais... l'algorithme aurait pu retourner
$$X - 1 \mod 13, \quad X - 2 \mod 13, \quad \mathbf{X + 10} \mod \mathbf{13}$$
ce qui aurait donné le produit $X^3 + 7X^2 - 28X + 20 \neq f$.

Conséquence : lorsqu'on injecte $\mathbb{F}_p[X] \to \mathbb{Z}[X]$, on choisit de prendre les coefficients entre $-p/2$ et $p/2$.

Question. Choisir $p > 2\,\|f\|_\infty$ suffit-il ?

Quelle taille pour p ? Exemples.

Exemple désagréable. Pour $f = X^{105} - 1$, on a le facteur premier suivant :

$$\begin{aligned} g = \; & X^{48} + X^{47} + X^{46} - X^{43} - X^{42} - 2X^{41} - X^{40} - X^{39} \\ & + X^{36} + X^{35} + X^{34} + X^{33} + X^{32} + X^{31} - X^{28} - X^{26} \\ & - X^{24} - X^{22} - X^{20} + X^{17} + X^{16} + X^{15} + X^{14} + X^{13} \\ & + X^{12} - X^{9} - X^{8} \mathbf{-2X^{7}} - X^{6} - X^{5} + X^{2} + X + 1 \end{aligned}$$

On a donc un facteur premier g de f dans $\mathbb{Z}[X]$, tel que $\|g\|_\infty = 2 > \|f\|_\infty = 1$.

On veut donc choisir p de sorte que $p/2$ soit plus grand que le plus grand coefficient d'un facteur propre quelconque de f.

Question. Peut-on majorer $\|g\|_\infty$ en fonctions de $\|f\|_\infty$?

Borne de Landau-Mignotte

Théorème [borne de Landau-Mignotte]. Soient A, B deux polynômes de $\mathbb{Z}[X]$ tels que B divise A. Si $B = \sum_{i=0}^{n} b_i X^i$ a degré n, alors

$$\|B\|_\infty := \max\{|b_i|, i \in \{0, \ldots, n\}\} \leq \binom{n}{\lfloor n/2 \rfloor} \|A\|_2$$

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

Preuve. Voir **[GG Chap 6.6]** ou **[AECF Chap 21]**. Fait intervenir la transformée de Fourier de fonction polynomiales dans $\mathbb{C}$.

Remarques.

- Si $n = 1$, on obtient une borne sur les racines de A dans $\mathbb{Z}$.
- La borne se relâche en l'expression plus simple $\|B\|_\infty \leq 2^n \sqrt{m+1}\, \|A\|_\infty$ où $m = \deg A$.

Choix de p

Revenons à notre algorithme.

1. On **élimine les facteurs carrés** dans f, en calculant $\mathrm{pgcd}(f, f')$.
2. On **choisit un « grand » nombre premier** p, respectant certaines conditions de divisibilité.
3. On calcule $g = f \bmod p$, puis une **factorisation de** g **dans** $\mathbb{Z}/p\mathbb{Z}$.
4. On **regroupe les facteurs** obtenus pour obtenir la factorisation dans $\mathbb{Z}[X]$.

Conséquence. À l'étape **2.**, on choisit $p/2 > B := 2^n \sqrt{n+1}\, \|f\|_\infty$.

D'**autres contraintes** pour p :

- p ne doit pas diviser le coefficient dominant de f,
- p doit laisser $(f \bmod p)$ sans carré.

Lemme. Soit $f \in \mathbb{Z}[X]$ sans carré. Alors $f \bmod p$ est sans carré si et seulement si p ne divise pas le discriminant $\mathrm{disc}(f) := \mathrm{res}(f, f')$.

On peut montrer qu'entre B et $2B$, il existe un premier p qui satisfait cette propriété, et il existe des algorithmes efficaces pour en trouver.

Plan

1. Quelques rappels

2. Factorisation dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$
   - Définition du problème
   - Élimination des facteurs carrés
   - Réduction à la factorisation dans $\mathbb{F}_p[X]$
   - Amélioration : lemme de Hensel
   - Dernière étape : regroupement des facteurs

3. Exercices

Taille de p

Problème. Les algorithmes de factorisation dans $\mathbb{F}_p[X]$ restent coûteux lorsque p suit la borne de Landau-Mignotte.

Idée. On factorise avec p plus petit, puis on essaie de remonter la factorisation dans $(\mathbb{Z}/p^k\mathbb{Z})[X]$, où p^k satisfait la borne de Landau-Mignotte.

Remarque. Le raisonnement est similaire à la recherche de racine carrées dans $(\mathbb{Z}/p^i\mathbb{Z})[X]$ (voir cours 3).

Lemme de Hensel

Lemme de Hensel (reformulé). Soit $P \in \mathbb{Z}[X]$ et $p \in \mathbb{Z}$ un nombre premier qui ne divise pas le coefficient dominant de P. Soit

$$P \equiv \lambda_1 A_1 B_1 \mod p$$

une factorisation de P dans $(\mathbb{Z}/p\mathbb{Z})[X]$, où $A_1, B_1 \in (\mathbb{Z}/p\mathbb{Z})[X]$ sont unitaires et premiers entre eux.

Alors, pour tout $i \geq 1$, il existe un **unique** couple de polynômes unitaires et premiers entre eux $A_i, B_i \in (\mathbb{Z}/p^i\mathbb{Z})[X]$ tels que

$$\begin{array}{rcll} P & \equiv & \lambda_i A_i B_i & \mod p^i \\ A_i & \equiv & A_1 & \mod p \\ B_i & \equiv & B_1 & \mod p \end{array}$$

Par ailleurs, pour tout $i \geq 1$, λ_i est le coefficient dominant de P modulo p^i.

Remarque. La preuve de ce résultat est constructive. Étant donnée une relation de Bezout $U_1 A_1 + V_1 B_1 = 1$ modulo p, on construit effectivement et successivement les relations $U_i A_i + V_i B_i$ modulo p^i.

Preuve

Éléments de preuve du lemme de Hensel.

Par hypothèse, $P = A_1 B_1$ dans $\mathbb{Z}/p\mathbb{Z}[X]$, avec $\mathrm{pgcd}(A_1, B_1) = 1$. Donc on peut calculer $U, V \in \mathbb{Z}/p\mathbb{Z}[X]$ tels que

$$UA_1 + VB_1 = 1\,.$$

Supposons que l'on ait le resultat à l'étape i, c'est-à-dire A_i et B_i ont été construits modulo p^i. Alors, on peut calculer $S \in \mathbb{Z}/p\mathbb{Z}$ tel que

$$P - \lambda_i A_i B_i = p^i S \mod p^{i+1}\,.$$

Cherchons maintenant des candidats pour A_{i+1} et B_{i+1}. On doit avoir

$$A_{i+1} \equiv A_i + p^i Q_A \mod p^{i+1} \quad \text{et} \quad B_{i+1} \equiv B_i + p^i Q_B \mod p^{i+1}$$

Puis,

$$A_{i+1}B_{i+1} \equiv A_i B_i + p^i (Q_A B_i + Q_B A_i) \equiv A_i B_i + p^i (Q_A B_1 + Q_B A_1) \mod p^{i+1}$$

Il résulte que $Q_A B_1 + Q_B A_1 \equiv S \mod p$. Autrement dit,

$$B_1 Q_A \equiv S \mod (p, A_1) \quad \Longrightarrow \quad Q_A \equiv (VB_1) Q_A \equiv VS \mod (p, A_1)$$

Conclusion partielle (unicité si existence). Nécessairement, $A_{i+1} = A_i + p^i Q_A$ où Q_A est le reste $VS \mod A_1$ dans $\mathbb{F}_p[X]$. De même, $B_{i+1} = B_i + p^i Q_B$ où Q_B est le reste $US \mod B_1$ dans $\mathbb{F}_p[X]$.

Pour terminer la preuve, il reste à **vérifier** que ces choix de A_{i+1} et B_{i+1} conviennent *(laissé en exercice — raisonner sur les degrés)*.

Plan

1. Quelques rappels

2. Factorisation dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$
   - Définition du problème
   - Élimination des facteurs carrés
   - Réduction à la factorisation dans $\mathbb{F}_p[X]$
   - Amélioration : lemme de Hensel
   - Dernière étape : regroupement des facteurs

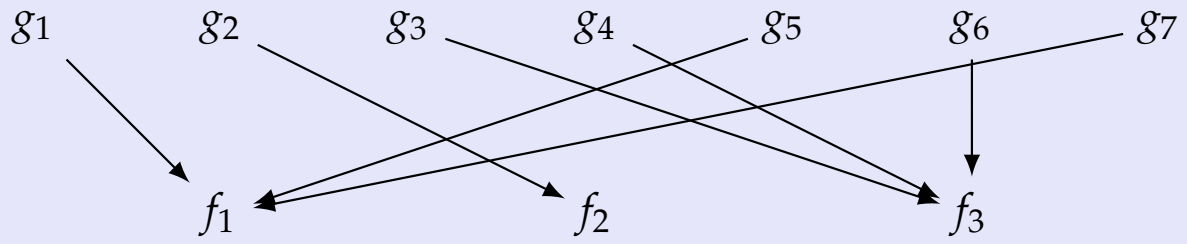
3. Exercices

Regroupement des facteurs

Résumé : on a effectué

$$f = f_1 \times \cdots \times f_k \quad \to \quad f \mod p \quad \to \quad (g_1 \mod p) \times \cdots \times (g_s \mod p)$$

But. Combiner les g_j pour retrouver les f_i.



Méthode simple : Calculer des produits entre g_i jusqu'à obtenir un polynôme irréductible dans $\mathbb{Z}[X]$ (test efficace).

Mais **le nombre d'appariements possibles est exponentiel en** s, qui peut être linéaire en le degré de f.

On peut raffiner avec les conditions sur le degré, mais cela reste **exponentiel** en pire cas.

Important. Pour rendre l'algorithme polynomial, il faut utiliser d'autres méthodes à base de **réduction de réseaux euclidiens** (algorithme LLL). Voir par exemple **[GG Chap 16.4 et 16.5]** ou **[AECF Chap 21.4]**.

Exemple final

But : factoriser $P = X^5 + 5X^4 + 19X^3 + 86X^2 + 39X + 2$ dans $\mathbb{Z}[X]$ avec la remontée de Hensel.

1. On a $P' = 5X^4 + 20X^3 + 57X^2 + 172X + 39$ et on vérifie que $\mathrm{pgcd}(P, P') = 1$.
2. On choisit $p = 5$ et on calcule P modulo p pour obtenir $Q = X^5 + 4X^4 + X^3 + 4X^2 + 2$.
3. L'algorithme de Berlekamp avec $p = 5$ retourne la factorisation
$$A_1 \cdot B_1 = (X^3 + 2X + 1) \cdot (X^2 + 2X + 2)$$
4. On détermine le p^k minimal pour lequel on doit remonter le résultat modulo p^k. La borne de Landau-Mignotte donne $\|P\|_2 \simeq 88.54$ puis $k = 6$.
   4.1 La première étape de la remontée de Hensel donne
   $$A_2 = X^2 - 20X + 2 \text{ et } B_2 = X^3 + 17X + 1 \qquad \bmod 25$$
   puis $A_2B_2 = X^5 - 20X^4 + 19X^3 - 339X^2 + 14X + 2 \neq P$.
   4.2 La seconde étape de la remontée de Hensel donne
   $$A_3 = X^2 + 5X + 2 \text{ et } B_3 = X^3 + 17X + 1 \qquad \bmod 125$$
   puis $A_3B_3 = X^5 + 5X^4 + 19X^3 + 86X^2 + 39X + 2 = P$.
   4.3 Les étapes suivantes donnent le même résultat (modulo 625, 3125, ...).

On obtient bien la factorisation voulue dans $\mathbb{Z}[X]$:

$$X^5 + 5X^4 + 19X^3 + 86X^2 + 39X + 2 = (X^2 + 5X + 2)(X^3 + 17X + 1)$$

Plan

1. Quelques rappels

2. Factorisation dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$
   Définition du problème
   Élimination des facteurs carrés
   Réduction à la factorisation dans $\mathbb{F}_p[X]$
   Amélioration : lemme de Hensel
   Dernière étape : regroupement des facteurs

3. Exercices

Exercice 1

Exercice [extrait de [LN 4.18]. Soit $\mathbb{F}_q$ un corps fini et ℓ un nombre premier divisant $q-1$. Soit également $a \in \mathbb{F}_q^*$. On souhaite montrer, à l'aide de l'algèbre de Berlekamp, que l'on a

$$X^\ell - a \text{ est irréductible dans } \mathbb{F}_q[X] \quad \Longleftrightarrow \quad a^{(q-1)/\ell} \neq 1\,.$$

Question 1. Soit $0 \leq i < \ell$. Calculer $X^{iq} \mod (X^\ell - a)$.

Question 2. En déduire que l'algèbre de Berlekamp peut être décrite comme

$$\mathcal{B} = \ker \phi = \Big\{ \sum_{i=0}^{\ell-1} b_i X^i \;\Big|\; b_i(a^{i(q-1)/\ell} - 1) = 0 \Big\}.$$

Question 3. À l'aide des questions précédentes, démontrer le résultat souhaité.

Exercice 1

Exercice [extrait de [LN 4.18]. Soit $\mathbb{F}_q$ un corps fini et ℓ un nombre premier divisant $q-1$. Soit également $a \in \mathbb{F}_q^*$.

Question 1. Soit $0 \leq i < \ell$. Calculer $X^{iq} \mod (X^\ell - a)$.

Question 2. En déduire que l'algèbre de Berlekamp peut être décrite comme

$$\mathcal{B} = \ker \phi = \Big\{ \sum_{i=0}^{\ell-1} b_i X^i \mid b_i(a^{i(q-1)/\ell} - 1) = 0 \Big\}.$$

Q1. On a

$$X^{iq} = X^{i(q-1)} X^i = (X^\ell)^{i(q-1)/\ell} X^i \equiv a^{i(q-1)/\ell} X^i = \left(a^{(q-1)/\ell} X\right)^i \mod (X^\ell - a)\,.$$

Q2. Rappelons que l'algèbre de Berlekamp $\mathcal{B}$ est le noyau de $\phi : B \mapsto B^q - B$ dans $\mathbb{F}_q[X]/(X^\ell - a)$. Pour $B \in \mathbb{F}_q[X]/(X^\ell - a)$, on calcule $B^q \mod (X^\ell - a)$:

$$B^q = \Big(\sum_{i=0}^{d} b_i X^i \Big)^q = \sum_{i=0}^{d} b_i^q X^{iq} \equiv \sum_{i=0}^{d} b_i a^{i(q-1)/\ell} X^i \mod (X^\ell - a)\,.$$

Donc

$$B \in \ker \phi \iff B^q - B \equiv 0 \mod (X^\ell - a) \iff \sum_{i=0}^{d} b_i (a^{i(q-1)/\ell} - 1) X^i \equiv 0 \mod (X^\ell - a)\,.$$

Comme $(1, \ldots, X^{\ell-1})$ est une base de $\mathbb{F}_q[X]/(X^\ell - a)$, on obtient

$$B \in \ker \phi \iff \forall i \in \{0, \ldots, \ell-1\},\ b_i(a^{i(q-1)/\ell} - 1) = 0\,.$$

Exercice 1

Exercice [extrait de [LN 4.18]. Soit $\mathbb{F}_q$ un corps fini et ℓ un nombre premier divisant $q-1$. Soit également $a \in \mathbb{F}_q^*$.

Question 3. À l'aide des questions précédentes, démontrer

$$X^\ell - a \text{ est irréductible dans } \mathbb{F}_q[X] \quad \iff \quad a^{(q-1)/\ell} \neq 1\,.$$

Q3. On a vu dans le cours l'équivalence

$$X^\ell - a \text{ irréductible} \iff \text{algèbre de Berlekamp } \mathcal{B} = \mathbb{F}_q$$

D'après **Q2.**, $\mathcal{B} = \left\{ \sum_{i=0}^{\ell-1} b_i X^i \mid b_i(a^{i(q-1)/\ell} - 1) = 0 \right\}$, donc

$$X^\ell - a \text{ irréductible} \iff \forall i \in \{1, \ldots, \ell-1\},\ a^{i(q-1)/\ell} - 1 \neq 0\,.$$

Remarquons enfin que, pour $i \in \{1, \ldots, \ell-1\}$ fixé, on a

$$a^{i(q-1)/\ell} \neq 1 \iff a^{(q-1)/\ell} \neq 1,$$

car l'ordre de $a^{(q-1)/\ell}$ doit être un diviseur de ℓ, qui est premier. Ceci conclut la preuve.

Exercice 2

But : traiter le cas où $q = 2^k$ dans les algorithmes de Berlekamp et Cantor-Zassenhaus.

Rappel : dans le cas q impair, on a utilisé le fait qu'exactement la moitité des éléments non-nuls sont des carrés dans $\mathbb{F}_{q'}$.

Exercice [extrait de GG 14.16]. Soit $q = 2^k$ et, pour $m \in \mathbb{N}$ quelconque et

$$T_m : x \mapsto x^{2^{m-1}} + x^{2^{m-2}} + \cdots + x^2 + x\,.$$

Question 1. Démontrer que pour tout $u \in \mathbb{F}_q[X]$, on a $u^{2^m} + u = T_m(u) \cdot (T_m(u) + 1)$.

Question 2. Démontrer que si $\alpha \in \mathbb{F}_{2^m}$, alors $T_m(\alpha) \in \mathbb{F}_2$. En déduire que si α est choisi uniformément dans $\mathbb{F}_{2^m}$, alors $T_m(\alpha)$ est uniforme dans $\mathbb{F}_2$.

Soit P est un polynôme de $\mathbb{F}_q[X]$ sans facteur carré, donc les facteurs premiers sont $P_1, \ldots, P_r$. On note $\chi_i(F) = F \mod P_i$.

Question 3. [Berlekamp] Démontrer que pour tout B dans l'algèbre de Berlekamp $\mathcal{B}$, on a $\chi_i(T_k(B)) \in \mathbb{F}_2$. En déduire que si B est tiré uniformément dans $\mathcal{B}$, alors $T_k(B) \in \mathbb{F}_2$ avec probabilité 2^{1-r}.

Question 4. [Cantor-Zassenhaus] On suppose que les P_i ont même degré d. Démontrer que pour tout $A \in \mathbb{F}_q[X]/(P)$, on a $\chi_i(T_{kd}(A)) \in \mathbb{F}_2$. En déduire que si A est tiré uniformément dans $\mathbb{F}_q[X]/(P)$, alors $T_{kd}(A) \in \mathbb{F}_2$ avec probabilité 2^{1-r}.

Exercice 2

Exercice [extrait de GG 14.16]. Soit $q = 2^k$ et, pour $m \in \mathbb{N}$ quelconque et

$$T_m : x \mapsto x^{2^{m-1}} + x^{2^{m-2}} + \cdots + x^2 + x\,.$$

Question 1. Démontrer que pour tout $u \in \mathbb{F}_q[X]$, on a $u^{2^m} + u = T_m(u) \cdot (T_m(u) + 1)$.

Question 2. Démontrer que si $\alpha \in \mathbb{F}_{2^m}$, alors $T_m(\alpha) \in \mathbb{F}_2$. En déduire que si α est choisi uniformément dans $\mathbb{F}_{2^m}$, alors $T_m(\alpha)$ est uniforme dans $\mathbb{F}_2$.

Q1.

$$T_m(u)^2 = (u^{2^{m-1}} + u^{2^{m-2}} + \cdots + u^2 + u)^2 = u^{2^m} + u^{2^{m-1}} + \cdots + u^4 + u^2.$$

Donc

$$T_m(u)(T_m(u) + 1) = T_m(u)^2 + T_m(u) = u^{2^m} + u$$

Q2. Si $\alpha \in \mathbb{F}_{2^m}$, alors $\alpha^{2^m} + \alpha = 0$, donc $T_m(\alpha)^2 = T_m(\alpha)$. Cela signifie que $T_m(\alpha) \in \mathbb{F}_2$. Par ailleurs, $T_m : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ est $\mathbb{F}_2$-linéaire, donc

$$|\{\alpha \in \mathbb{F}_{2^m}, T_m(\alpha) = 0\}| = |\ker T_m| = 2^{\dim \ker \phi} = 2^{m - \mathrm{rk}\phi} = 2^{m-1}\,.$$

Si α est tiré uniformément dans $\mathbb{F}_{2^m}$, alors $T_m(\alpha) = 0$ avec probabilité $2^{m-1}/2^m = 1/2$.

Exercice 2

Soit P est un polynôme de $\mathbb{F}_q[X]$ sans facteur carré, donc les facteurs premiers sont $P_1, \ldots, P_r$. On note $\chi_i(F) = F \mod P_i$.

Question 3. [Berlekamp] Démontrer que pour tout B dans l'algèbre de Berlekamp $\mathcal{B}$, on a $\chi_i(T_k(B)) \in \mathbb{F}_2$. En déduire que si B est tiré uniformément dans $\mathcal{B}$, alors $T_k(B) \in \mathbb{F}_2$ avec probabilité 2^{1-r}.

Q3. Soit $B \in \mathcal{B}$. On rappelle que, par définition de l'algèbre de Berlekamp, pour tout i on a

$$\chi_i(B) = B \mod P_i \in \mathbb{F}_{2^k}.$$

Comme les opérateurs T_k et χ_i commutent, il résulte que $\chi_i(T_k(B)) = T_k(\chi_i(B)) \in \mathbb{F}_2$.

D'après le théorème des reste chinois, on a $T_k(B) = 0$ si $\chi_i(T_k(B)) = 0$ pour tout i, et $T_k(B) = 1$ si $\chi_i(T_k(B)) = 1$ pour tout i. Autrement dit, $T_k(B) \in \mathbb{F}_2$ si (et seulement si) les $\chi_i(T_k(B))$ sont tous égaux.

Par ailleurs, les variables $\{\chi_i(T_k(B))\}$ sont indépendantes, donc lorsque B est tiré uniformément, on a d'après la **Q2.** :

$$\mathbb{P}\left[\chi_1(T_k(B)) = \cdots = \chi_r(T_k(B))\right] = 2 \times \frac{1}{2^r} = 2^{1-r}.$$

Remarque. L'algorithme de Berlekamp en grande cardinalité échoue quand $T_k(B) \in \mathbb{F}_2$. On a montré que cette probabilité est $\leq 1/2$.

Exercice 2

Question 4. [Cantor-Zassenhaus] On suppose que les P_i ont même degré d. Démontrer que pour tout $A \in \mathbb{F}_q[X]/(P)$, on a $\chi_i(T_{kd}(A)) \in \mathbb{F}_2$. En déduire que si A est tiré uniformément dans $\mathbb{F}_q[X]/(P)$, alors $T_{kd}(A) \in \mathbb{F}_2$ avec probabilité 2^{1-r}.

Q4. Comme les P_i ont degré d, on sait que $\mathbb{F}_q[X]/(P_i)$ est isomorphe à $\mathbb{F}_{q^d} = \mathbb{F}_{2^{kd}}$.
En utilisant la **Q2.** avec $m = kd$, on obtient $\chi_i(T_{kd}(A)) = T_{kd}((\chi_i(A)) \in \mathbb{F}_2$.

Puis, on répète le raisonnement de la **Q3.**. D'après le théorème des reste chinois, $T_{kd}(A) \in \mathbb{F}_2$ si (et seulement si) les $\chi_i(T_k(A))$ sont tous égaux.

Par ailleurs, les variables $\{\chi_i(T_k(A))\}$ sont indépendantes, donc lorsque A est tiré uniformément, on a d'après la **Q2.**

$$\mathbb{P}\left[\chi_1(T_{kd}(A)) = \cdots = \chi_r(T_{kd}(B))\right] = 2 \times \frac{1}{2^r} = 2^{1-r}.$$

Remarque. L'algorithme de Cantor-Zassenhaus échoue quand $T_{kd}(B) \in \mathbb{F}_2$. On a montré que cette probabilité est $\leq 1/2$.