Algorithme de Berlekamp

Leçon : 123, 141, 151, 142, 122

Rég : Objectif Agrégation

But : décomposer en facteurs irréductibles un polynôme sans facteurs carrés à coefficients dans un corps.

Lemme Soient p 1er, $n \in \mathbb{N}^*$, $q = p^n$ et $R \in \mathbb{F}_q[X]$. L'application

$$S_R : \begin{cases} \mathbb{F}_q[X]/(R) \to \mathbb{F}_q[X]/(R) \\ \Phi \bmod R \mapsto \Phi(X^q) \bmod R \end{cases}$$

est bien définie et coïncide avec l'élévation à la puissance q dans $\mathbb{F}_q[X]/(R)$.

Démonstration

On pose le morphisme d'anneaux $\sigma_1 : \mathbb{F}_q[X] \to \mathbb{F}_q[X]$, $\Phi(X) \mapsto \Phi(X^q)$.

On a $\sigma_1(\Phi) \overset{\text{def}}{=} \Phi(X^q) = \Phi^p$ (↑ morphisme de Frobenius).

Soit $\pi : \mathbb{F}_q[X] \twoheadrightarrow \mathbb{F}_q[X]/(R)$ la projection, et $\sigma = \pi \circ \sigma_1$.

π morphisme donc $\sigma(R) = \pi(R)^q = 0$. Donc $(R) \subset \ker \sigma$, σ passe au quotient par (R) et donne S_R. Donc S_R bien définie.

Vérifions que S_R coïncide avec l'élévation à la puissance q modulo R.

$S_R(\Phi \bmod R) = S_R(\pi(\Phi)) = \pi(\Phi(X^p)) = \pi(\Phi^p) = \pi(\Phi)^p$. □

On considère les $\mathbb{F}_q$-espaces vectoriels de dim finie $K_i = \mathbb{F}_q[X]/(P_i)$, où $P = \prod_{i=1}^{n} P_i$, décomposition en irréductibles sans facteurs carrés.

Les P_i sont irréd., donc K_i sont des corps. Par le théorème chinois on a l'isomorphisme de $\mathbb{F}_q$-algèbres :

$$\varphi : \begin{cases} \mathbb{F}_q[X]/(P) \to K_1 \times \cdots \times K_n \\ \Phi \bmod P \mapsto (\Phi \bmod P_1, \ldots, \Phi \bmod P_n) \end{cases}$$

(les P_i sont 2 à 2 1er entre eux).

Théorème (algorithme) Soit $P \in \mathbb{F}_q[X]$ un polynôme dont la décomposition en facteurs irréductibles est connue. On pose $\mathcal{A} = X \bmod P$ dans $\mathbb{F}_q[X]/(P)$, et on considère dans la base $\mathcal{B} = \{1, \mathcal{A}, \dots, \mathcal{A}^{\deg P - 1}\}$ de $\mathbb{F}_q[X]/(P)$. Alors le processus suivant s'arrête au bout d'un nbre fini d'étapes :

① On calcule $\mathrm{Mat}_{\mathcal{B}}(S_p - Id)$

② Le nbre de facteurs irréductibles de P est :

$$r = \dim(\ker(S_p - Id)) = \deg(P) - \mathrm{rg}(S_p - Id)$$

Si $r = 1$: P irréd., on arrête.

③ On calcule un polynôme V non constant de $\mathbb{F}_q[X]$ modulo P et tel que $V^q \bmod P \in \ker(S_p - Id)$. On calcule avec l'algo d'Euclide pour $\gcd(P, V - \alpha)$, on a alors :

$$P = \prod_{\alpha \in \mathbb{F}_q} \gcd(P, V - \alpha)$$

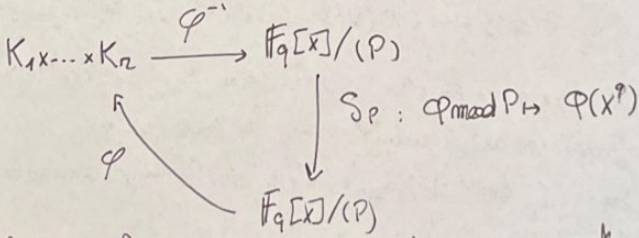
On retourne au ① avec chacun des facteurs non triviaux de ce produit.

Démonstration

Soit $P = P_1 \cdots P_n$ la décomposition de P en polynômes irréductibles $\neq$ deux à deux.

Rq $r = \dim(\ker(S_p - Id))$.

On pose $\tilde{S_p} := \varphi \circ S_p \circ \varphi^{-1} : K_1 \times \cdots \times K_n \to K_1 \times \cdots \times K_n$.



$\tilde{S_p}$ est l'élévation à la puissance q composante par composante.

Donc : $(x_1, \dots, x_n) \in \ker(\tilde{S_p} - Id) \iff (x_1^q, \dots, x_n^q) = (x_1, \dots, x_n)$

$\iff \forall i \in [\![1, n]\!]$, $x_i^q = x_i$ dans K_i.

Or pour $i \in [\![1, r]\!]$:

$$\alpha_i = \alpha \iff \overline{V-\alpha}^{\,i} = 0$$

$$\iff P_i \mid V-\alpha.$$

Donc $I_\alpha = \{ i \in [\![1, r]\!] : \alpha_i = \alpha \}$ et donc $\mathrm{pgcd}(P, V-\alpha) = \prod_{\{i, \alpha_i = \alpha\}} P_i$.

Ainsi : $P = \prod_{i=1}^{r} P_i = \prod_{\alpha \in \mathbb{F}_q} \left(\prod_{\{i, \alpha_i = \alpha\}} P_i \right) \overset{(*)}{=} \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V-\alpha)$.

Vérifions que l'algorithme termine, ie que r diminue strictement.

Si V non congru à un polynôme constant modulo P, il existe $i, j \in [\![1, r]\!]$ tq $\alpha_i \neq \alpha_j$.

[En effet, si $\forall i, j \in [\![1, r]\!]$, $\alpha_i = \alpha_j$, on aurait $\overline{V}$ constant par le théorème chinois.

Ainsi, dans $(*)$ au moins deux facteurs sont non triviaux. $\left(\prod_{\{k, \alpha_k = \alpha_i\}} P_k \neq \prod_{\{k, \alpha_k = \alpha_j\}} P_k \right)$

De plus, ils sont bien sans facteurs carrés. ■

En pratique : calcul de pgcd : algorithme d'Euclide de rang, pivot de Gauss.) à savoir pour la complexité.

$\to o(\deg(P)^3)$.

$\to q$ calcul de pgcd, $\deg(P)$ étape de calcul.

et une division par X en $\deg(P)$

$$\Rightarrow O(\deg(P)^3 + q \deg(P)^2).$$

On considère une extension $\mathbb{F}_q \hookrightarrow K$ du corps $\mathbb{F}_q$. L'image de $\mathbb{F}_q$ dans K est l'ensemble des éléments de K vérifiant $x^q = x$.

En effet : • si $x \in \mathbb{F}_q^\times$, par le théorème de Lagrange $x^{q-1} = 1$, donc $x^q = x$ et c'est aussi vrai pour $x = 0$, donc $\forall x \in \mathbb{F}_q$, $x^q = x$.

• le polynôme $X^q - X \in K[X]$ est de degré q et admet déjà q racines, il n'y a pas d'autre élément dans K vérifiant l'équation $X^q = X$.

Ainsi : $(x_1, \dots, x_n) \in \mathrm{Ker}(\tilde{S}_p - \mathrm{Id}) \iff \forall i \in [\![1, n]\!]$ $x_i \in \mathbb{F}_q \hookrightarrow K$,

donc $\mathrm{Ker}(\tilde{S}_p - \mathrm{Id}) = (\mathbb{F}_q)^n$. On $\mathrm{Ker}(\tilde{S}_p - \mathrm{Id}) = \mathcal{P}(\mathrm{Ker}(S_p - \mathrm{Id}))$.

Comme $\mathcal{P}$ est un isomorphisme de $\mathbb{F}_q$-ev, donc $\dim(\mathrm{Ker}(S_p - \mathrm{Id})) = n$.

* Supposons que $n > 1$.

On note $\bar{U}$ la classe de $U \in \mathbb{F}_q[X]$ dans $\mathbb{F}_q[X]/(P)$.

$\bar{U}^i$ ——— $U \in \mathbb{F}_q[X]$ ——— $\mathbb{F}_q[X]/(P_i)$.

On remarque $\{\bar{U},$ tq $\bar{U}$ constant$\} = \mathrm{Vect}\{1\}$ dans $\mathbb{F}_q[X]/(P)$.

On $\dim(\mathrm{Ker}(S_p - \mathrm{Id})) = n > 1$, donc il existe $V \in \mathbb{F}_q[X]$ tq $\bar{V}$ non constant et $\bar{V} \in \mathrm{Ker}(S_p - \mathrm{Id}) \iff (\bar{V}^1, \dots, \bar{V}^n) \in (\mathbb{F}_q)^n$.

Pour tout $i \in [\![1, n]\!]$, on note $\alpha_i = \bar{V}^i \in \mathbb{F}_q \subset K_i$.

• Mq $\forall \alpha \in \mathbb{F}_q$ $\mathrm{pgcd}(P, V - \alpha) = \prod_{\{i, \alpha_i = \alpha\}} P_i$.

$\mathrm{pgcd}(P, V-\alpha) \mid P$, donc il est de la forme $\prod_{i \in I_\alpha} P_i$, $I_\alpha \subset [\![1, n]\!]$.

Par le théorème de Gauss, comme les polynômes sont 2 à 2 premiers entre eux :

$I_\alpha = \{i \in [\![1, n]\!] : P_i \mid V - \alpha\}$.

En effet : $\prod_{i, P_i \mid V-\alpha} P_i \mid V - \alpha$ et $\prod_{i, P_i \mid V-\alpha} P_i \mid P$ (théorème de Gauss) donc $\prod_{i, P_i \mid V-\alpha} P_i \mid \prod_{i \in I_\alpha} P_i$

donc $\{i \in [\![1, n]\!] : P_i \mid V - \alpha\} \subset I_\alpha$. Et si $i \in I_\alpha$, alors $P_i \mid \prod_{j \in I_\alpha} P_j \mid V - \alpha$.

On peut en déduire un algorithme factorisant les polynômes sur les corps finis.

Il faut revenir au $P \in \mathbb{F}_q[X]$ a des facteurs carrés ou non.

On énonce quelques résultats.

Lemme Soit K corps fini, $\mathrm{car}(K) = p$, $P \in K[X]$.

$P' = 0 \iff \exists R \in K[X],\ P = R^p$ ⚠ $P' = 0$ ⇏ P carré.

Proposition : $\mathrm{pgcd}(P, P')$

i) Soit K corps, $\mathrm{car}(K) = 0$. Soit $P \in K[X]$, et $Q \in K[X]$ un facteur irréductible de P de multiplicité μ. Alors Q est un facteur irréductible de $\mathrm{pgcd}(P, P')$ de multiplicité $\mu - 1$.

Si $P = \prod_{i=1}^{m} P_i^{\ell_i}$, P_i 2 à 2 1er entre eux,

$$\mathrm{pgcd}(P, P') = \prod_{i=1}^{m} P_i^{\ell_i - 1}.$$

ii) Si $\mathrm{car}(K) = p$, K corps fini, Q irréd. Q est un facteur irréductible de $\mathrm{pgcd}(P, P')$ de multiplicité μ^*, où

$$\mu^* = \begin{cases} \mu - 1 \text{ si } p \nmid \mu \\ \mu \text{ ou } p \mid \mu \end{cases}$$

Si $P = \prod_{i=1}^{m} P_i^{\ell_i}$, $\mathrm{pgcd}(P, P') = \left(\prod_{p \mid \ell_i} P_i^{\ell_i}\right)\left(\prod_{p \nmid \ell_i} P_i^{\ell_i - 1}\right)$

→ cf Objectif Agreg

ex. $P(X) = X^p(X+1)$. $Q = X^p$ ⇏, $\mathrm{pgcd}(P, P') = P' = X^p$.

$P'(X) = X^p$ $\quad Q = X+1$, → ok

App. $\text{pgcd}(P,P')=1 \iff P$ sans facteurs carrés.

Si $R=\mathbb{F}_q$, $q=p^n$, $\text{pgcd}(P,P')=P \iff P'=0$

$\iff \exists R \in \mathbb{F}_q[X]$ $P=R^p$.

→ on en déduit Bal générale.

Exemple d'application.

- $P(X)=X^2+1 \in \mathbb{F}_3[X]$ $\alpha = X \bmod P$

→ P sans carré.

→ $P'=2X$, $\text{pgcd}(P,P')=1$, P sans facteur carré.

Bale Ramp. $\alpha^2=1$.

$\begin{cases} Sp(1)=1 \\ Sp(\alpha)=\alpha^3=\alpha\times\alpha^2=\alpha \end{cases}$ $\Rightarrow \text{Mat}_{1,\alpha}(Sp-Id)=0$

$\Rightarrow r=2$.

On prend $V(X)=X$.

$P=\text{pgcd}(P,V)\,\text{pgcd}(P,V-1)\,\text{pgcd}(P,V+1)$

$=(X-1)(X+1)$.

- $P=X^2-1 \in \mathbb{F}_2[X]$ $P'=0$, $R=(X-1)$, $P=R^2$.

→ Bale Ramp ⊘ R.