ALGORITHME DE BERLEKAMP

Leçons : 123, 141, 151

Référence Objectif agrégation p. 244.

Algorithme

Soit $P \in \mathbb{F}_q[X]$, avec $q = p^s$ où p premier et $s \in \mathbb{N}^*$.

tel que $P = \prod_{i=1}^{r} P_i$ où les P_i sont irréductibles et distincts

(i.e. P n'a pas de facteur carré)

On peut factoriser P ainsi :

1 - Calcul du nombre d'irréductibles r de P :

$$r = \dim \operatorname{Ker}(S_p - Id)$$

où S_p : $\mathbb{F}_q[X]/\langle P \rangle \longrightarrow \mathbb{F}_q[X]/\langle P \rangle$, $Q(X) \bmod P \longmapsto Q(X^q) \bmod P$. est linéaire (!)

→ Si $r = 1$ on a gagné.

2 - Calcul d'un polynôme V non congru modulo P à un polynôme constant de $\mathbb{F}_q[X]$ et tel que $V \bmod P \in \operatorname{Ker}(S_p - Id)$.

On a alors $P = \prod_{\alpha \in \mathbb{F}_q} \operatorname{PGCD}(P, V - \alpha)$

Et on recommence sur les facteurs non triviaux de ce produit.

Résumé

I - Définition et linéarité de S_p.

II - Calcul de $r = \dim(\operatorname{Ker}(S_p - Id))$.

III - Factorisation de P.

IV - Terminaison de l'algorithme

I | • Posons $\delta_1 : \mathbb{Q}(X) \longrightarrow \mathbb{Q}(X^q)$

C'est l'unique morphisme d'anneau tel que $\delta_1(a) = a$ pour $a \in \mathbb{F}_q$

$\delta_1(X) = X^q$

Mais dans $\mathbb{F}_q$, $a^q = a$, on a donc : $\delta_1(Q) = Q(X^q) = Q^q$.

Posons alors $\pi : \mathbb{F}_q[X] \longrightarrow \mathbb{F}_q[X]/\langle P \rangle$ la surjection canonique.

on a alors $\pi \circ \delta_1(P) = \pi(P^q) = \pi(P)^q = 0$.

on peut donc passer au quotient et définir :

$$\begin{array}{rccc} \delta_R : & \mathbb{F}_q[X]/\langle P \rangle & \longrightarrow & \mathbb{F}_q[X]/\langle P \rangle \\ & Q \bmod P & \longmapsto & Q(X^q) \bmod P \end{array}$$

et c'est un morphisme d'algèbre qui coïncide avec l'élévation à la puissance q car :

$$\delta_R(\pi(Q)) = \pi \circ \delta_1(Q) = \pi(Q^q) = (\pi(Q))^q.$$

II | • Considérons les $\mathbb{F}_q$-espaces vectoriels $K_i := \mathbb{F}_q[X]/\langle P_i \rangle$, ce sont des corps car les P_i sont irréductibles.

Et le théorème chinois donne l'isomorphisme d'algèbres :

$$\begin{array}{rccc} \varphi : & \mathbb{F}_q[X]/\langle P \rangle & \longrightarrow & K_1 \times \cdots \times K_r \\ & Q \bmod P & \longmapsto & (Q \bmod P_1, \ldots, Q \bmod P_r) \end{array}$$

car les P_i sont premiers deux à deux.

• On peut alors conjuguer S_p par φ : $\tilde{S}_p = \varphi \circ S_p \circ \varphi^{-1}$, et cette application est l'élévation à la puissance q dans $K_1 \times \cdots \times K_r$.

Donc $(x_1, \ldots, x_r) \in \ker(\tilde{S}_p - Id)$ ssi $(x_1^q, \ldots, x_r^q) = (x_1, \ldots, x_r)$

ie $x_i^q = x_i$ dans K_i.

• Mais on remarque que $\mathbb{F}_q \subseteq K_i$, et comme K_i est un corps, le polynôme $X^q - X$ a au plus q racines.

Or les éléments de $\mathbb{F}_q$ sont racines ! Ce sont donc les seules.

Donc $(x_1,\dots,x_r) \in \operatorname{Ker} \widetilde{S_p} - Id$ ssi $x_i \in \mathbb{F}_q$

ie $\operatorname{Ker}(\widetilde{S_p} - Id) = (\mathbb{F}_q)^r$.

- Mais on remarque que $\operatorname{Ker}(\widetilde{S_p} - Id) = \varphi(\operatorname{Ker} S_p - Id)$

donc comme φ est un isomorphisme :

$\dim \operatorname{Ker}(S_p - Id) = \dim \operatorname{Ker}(\widetilde{S_p} - Id) = \dim \mathbb{F}_q^{\,r} = r$.

III | • Supposons $r > 1$.

- Comme l'ensemble des $U \bmod P$ constants est la droite vectorielle engendrée par 1, et que $r > 1$, il existe

$V \bmod P \in \operatorname{Ker}(S_p - Id)$ non constant.

- Mais cela signifie en fait que $\alpha_i := V \bmod P_i \in \mathbb{F}_q \ (\subset K_i)$.

Dès lors, pour $\alpha \in \mathbb{F}_q$,

$\mathrm{PGCD}(P, V-\alpha)$ divise P donc est de la forme $\prod_{i \in I_\alpha} P_i$

où $I_\alpha = \left\{ i \in [\![1,r]\!] \;\middle|\; P_i \mid V-\alpha \right\}$

Or par définition de α_i,

$\alpha_i = \alpha$ ssi $V - \alpha = 0 \bmod P_i$ ssi $P_i \mid V-\alpha$.

C'est-à-dire : $\mathrm{PGCD}(P, V-\alpha) = \prod_{\{i,\, \alpha_i = \alpha\}} P_i$

- On conclut en écrivant :

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

IV | • Finalement, il ne reste plus qu'à s'assurer que l'algorithme termine.

• Comme $V \bmod P$ n'est pas constant, c'est bien une vraie factorisation car il existe alors $\alpha_i \neq \alpha_j$ pour un certain couple (i,j).

En effet, on aurait sinon $V = \alpha \bmod P_i$ pour tout i

donc $V = \alpha \bmod P$.

Remarques

• En pratique, pour calculer $\dim \mathrm{Ker}(Sp - Id)$, on doit calculer la matrice de $Sp - Id$ dans une base, par exemple $(1, x, \dots, x^{\deg P - 1})$ où $x = X \bmod P$, puis calculer son rang par Pivot de Gauss.

• Et pour calculer les PGCD, on utilise l'algorithme d'Euclide.

• On peut se débarasser des facteurs multiples en regardant $\mathrm{PGCD}(P, P')$, mais en caractéristique non nulle ce n'est pas si confortable.

→ si $P \wedge P' = 1$ c'est bon

→ si $P \wedge P' = P$ (ie $P' = 0$ dans $\mathbb{F}_q$), il existe R tel que $P = R^q$ et on applique l'algo à R.

→ sinon, $P_1 = \mathrm{PGCD}(P, P')$ ~~et $P_2 = \mathrm{PGCD}($~~

et $P_2 = P / \mathrm{PGCD}(P, P')$

sont deux facteurs non triviaux de P, et on peut itérer dessus !