Développement : Algorithme de Berlekamp

Leçons : 123, 141, 151.

Théorème. *Soient p premier, $q = p^s, P \in \mathbb{F}_q[X]$ sans facteurs carrés. Soient $d = \deg(P), x = X \pmod P$ dans $\mathbb{F}_q[X]/(P)$, soit $\mathcal{B} = (1, x, \cdots, x^{d-1})$ base de $\mathbb{F}_q[X]/(P)$. On considère l'application $S_P \left\{ \begin{array}{ll} \mathbb{F}_q[X]/(R) & \to \mathbb{F}_q[X]/(R) \\ \overline{Q} & \mapsto \overline{Q^q} \end{array} \right.$.*
C'est un morphisme d'anneaux et une application linéaire. On considère l'algorithme suivant :

1. *Calculer la matrice de $S_P - \mathrm{Id}$ dans $\mathcal{B}$, et calculer $r = \dim(\ker(S_P - \mathrm{Id})) = \deg(P) - \mathrm{rg}(S_P - \mathrm{Id})$. Si $r = 1$, on retourne P, sinon on passe en 2.*
2. *On calcule $V \in \mathbb{F}_q[X]$ tel que sa classe modulo P ne soit pas représentée par un polynôme constant, et tel que $\overline{V} \in \ker(S_P - \mathrm{Id})$. On calcule, pour $\alpha \in \mathbb{F}_q, \mathrm{pgcd}(P, V - \alpha)$ avec l'algorithme d'Euclide, et on retourne en 1 avec chacun des polynômes non triviaux obtenus.*

Cet algorithme termine et retourne la décomposition de P en facteurs irréductibles.

Démonstration.
On écrit $P = P_1 \cdots P_r$ la décomposition en produit d'irréductibles deux à deux distincts.
Pour tout i, on pose $K_i = \mathbb{F}_q[X]/(P_i)$. Soit $\varphi \left\{ \begin{array}{ll} \mathbb{F}_q[X]/(P) & \to K_1 \times \cdots \times K_r \\ Q \bmod P & \mapsto (Q \bmod P_1, \cdots, Q \bmod P_r) \end{array} \right.$.
C'est un isomorphisme (théorème chinois).

Étape 1 : $r = \dim(\ker(S_P - \mathrm{Id}))$.
On pose $\widetilde{S_P} = \varphi \circ S_P \circ \varphi^{-1} : K_1 \times \cdots K_r \to K_1 \times \cdots \times K_r$, qui correspond à l'élévation à la puissance q composante par composante. Ainsi $(x_1, \cdots, x_r) \in \ker(\widetilde{S_P} - \mathrm{Id}) \Leftrightarrow \forall i \in [\![1, r]\!], x_i^q = x_i$ dans K_i.
Soit $K/\mathbb{F}_q$ extension de corps. Alors l'image de $\mathbb{F}_q$ est l'ensemble des racines de $X^q - X$ dans $\mathbb{K}$: en effet, par Lagrange, tous les éléments de $\mathbb{F}_q^*$ sont racines, et 0 l'est aussi, et comme ce polynôme a au plus q racines, il y a égalité des ensembles. Ainsi $(x_1, \cdots, x_r) \in \ker(\widetilde{S_P} - \mathrm{Id}) \Leftrightarrow \forall i, x_i^q = x_i \Leftrightarrow x_i \in \mathbb{F}_q$ (vu comme sous-corps de K_i). Ainsi $\ker(\widetilde{S_P} - \mathrm{Id})$ isomorphe à $\mathbb{F}_q^r$, donc $\dim(\ker(S_p - \mathrm{Id})) = \dim(\ker(\widetilde{S_P} - \mathrm{Id})) = r$.

Étape 2 : Si $r > 1$, alors $P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V - \alpha)$.
On remarque que le sous-espace de $\mathbb{F}_q[X]/(P)$ formé des polynômes congrus à un polynôme constant est de dimension 1, engendré par $\overline{1}$. Comme $\dim(\ker(S_P - \mathrm{Id})) = r > 1$, il existe V non congru à un polynôme constant, tel que $V \pmod P \in \ker(S_P - \mathrm{Id})$. On a alors $\overline{V} \in \ker(S_P - \mathrm{Id}) \Leftrightarrow (V \pmod{P_1}, \cdots, V \pmod{P_r}) \in \mathbb{F}_q^r$. Pour tout $i \in [\![1, r]\!]$, soit $\alpha_i = V \pmod{P_i} \in \mathbb{F}_q \subset K_i$. Pour $\alpha \in \mathbb{F}_q$, montrons que $\mathrm{pgcd}(P, V - \alpha) = \prod_{\alpha_i = \alpha} P_i$. Comme $\mathrm{pgcd}(P, V - \alpha)$ divise P, il est de la forme $\prod_{i \in I_\alpha} P_i$. Les (P_i) étant deux à deux premiers entre eux, on a $I_\alpha = \{i \in [\![1, r]\!], P_i | (V - \alpha)\}$.
Mais $P_i | V - \alpha \Leftrightarrow V - \alpha = 0 \pmod{P_i} \Leftrightarrow \alpha_i = \alpha$. D'où $\mathrm{pgcd}(P, V - \alpha) = \prod_{\alpha_i = \alpha} P_i$.
Il s'ensuit que $P = \prod_{i=1}^{r} P_i = \prod_{\alpha \in \mathbb{F}_q} \left(\prod_{\alpha_i = \alpha} P_i \right) = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V - \alpha)$.

Étape 3 : L'algorithme termine.
Comme, par construction, à chaque étape V n'est pas congru à un polynôme constant modulo P, il existe $i \neq j$ tels que $\alpha_i \neq \alpha_j$. Ainsi, dans la décomposition précédente, au moins deux facteurs sont non triviaux, et comme P sans facteur carré, ils ont tous strictement moins de r facteurs irréductibles. Donc r diminue strictement à chaque itération. De plus, les $\mathrm{pgcd}(P, V - \alpha)$ étant diviseurs de P, ils sont aussi sans facteur carré. □

Notes personnelles

Savoir comment utiliser cet algorithme pour factoriser un polynôme ayant des facteurs carrés.

Références

V. Beck, J. Malick, G. Peyré, Objectif Agrégation, H&K, p. 244.