43 Algorithme de Berlekamp

ref : Beck On cherche à trouver tous les facteurs irréductibles de P, on peut le faire algorithmiquement grâce au théorème suivant.

THÉORÈME 43.1 *Soit $P \in \mathbb{F}_q[X]$ un polynôme sans facteur carré. On peut calculer le nombre de facteurs irréductibles et si il y en a plusieurs on peut trouver effectivement (algorithmiquement) un polynôme $V \in \mathbb{F}_q[X]$ tel que V soit non constant modulo P et :*

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

PREUVE. Remarquons que si V est non constant modulo P, $\operatorname{pgcd}(P, V-\alpha)$ est un diviseur strict de P pour tout α, donc on a décomposé P en produit de facteurs de degré strictement plus petits, on peut alors itérer le procéder, jusqu'à tomber sur les facteurs irréductibles.

$\mathbb{F}_q[X]$ est une $\mathbb{F}_q$-algèbre et (P) est un idéal de cette algèbre, donc on peut quotienter : $R = \mathbb{F}_q[X]/(P)$ est encore une $\mathbb{F}_q$-algèbre. L'élévation à la puissance q dans cette algèbre est $\mathbb{F}_q$ linéaire d'après le morphisme de Frobenius : $(x+y)^q = x^q + y^q$ et $x^q = 1$ pour $x \in \mathbb{F}_q$. C'est donc un endomorphisme de $\mathbb{F}_q$-algèbres. L'ensemble de ses points fixes $\ker(\varphi - \mathrm{id})$ forme alors une sous-algèbre de R.

Grâce au lemme chinois, on peut décomposer l'algèbre R : si $P = P_1 \times \cdots \times P_r$ est la décomposition de P en facteurs irréductibles, comme P est dans facteur carré les P_i sont premiers entre eux deux à deux. On a donc l'isomorphisme ψ de $\mathbb{F}_q$-algèbres suivant :

$$R \to \mathbb{F}_q[X]/P_1 \times \cdots \times \mathbb{F}_q[X]/P_r$$

Chaque facteur est un corps car les P_i sont irréductibles.

On peut alors transporter l'endomorphisme de Frobenius par cet isomorphisme :

$$\tilde{\varphi} = \psi \circ \varphi \circ \psi^{-1}$$

L'endomorphisme $\tilde{\varphi}$ de $\mathbb{F}_q$-algèbre correspond à l'élévation à la puissance q sur chaque facteur, en effet :

$$\psi \circ \varphi \circ \psi^{-1}(x) = \psi(\psi^{-1}(x))^q = (\psi(\psi^{-1}(x)))^q = x^q$$

Comme chaque facteur est une extension de $\mathbb{F}_q$, on a $x^q = x \Leftrightarrow x \in \mathbb{F}_q$, en effet, les éléments de $\mathbb{F}_q$ vérifient l'équation (par Lagrange) et il n'y a que q solutions a une équation de degré q dans un corps. Donc $\ker(\tilde{\varphi} - \mathrm{id}) = \mathbb{F}_q^r$ et $r = \dim \ker(\tilde{\varphi} - \mathrm{id}) = \dim \ker(\varphi - \mathrm{id})$. Ce nombre se calcule donc par un programme d'algèbre linéaire (on écrit cet endomorphisme dans la base $(1, x, \ldots, x^{\deg P - 1})$ de $\mathbb{F}_q[X]/(P)$ et on réduit la matrice sous forme échelonnée par pivot).

Maintenant, si $r \geq 2$, comme la droite $\mathbb{F}_q.1$, on peut trouver $V \in \ker(S - \mathrm{id})$ non constant, c'est-à-dire $V^q - V \pmod P$ non constant.

On a alors $V \pmod{P_i} = \alpha_i \in \mathbb{F}_q$. Donc P_i divise $V - \alpha_i$, et donc $P = P_1 \ldots P_r$ divise $\prod \operatorname{pgcd}(P, (V - \alpha))$ comme les P_i sont premiers entre eux. Dans l'autre sens, les $\operatorname{pgcd}(P, (V-\alpha))$ sont premiers entre eux deux à deux et divisent tous P, donc le produit divise P. D'où l'égalité voulue :

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

Chaque facteur de ce produit est de degré strictement plus petit par ce qu'on a déjà remarqué, donc l'algorithme termine.

□

Remarque : Si P a des facteurs multiples, on prend :

$$\frac{P}{\text{pgcd}(P, P')}$$

qui est alors sans facteur carré.

Leçons concernées : corps finis, polynômes irréductibles.