Algorithme de Berlekamp

Achille Méthivier

Théorème 1. *Soit $q = p^n$, avec p nombre premier et pour deux polynômes (sur un corps quelconque) R et Q, on note $R \wedge Q$ leur pgcd. Soit $P \in \mathbb{F}_q[X]$ qu'on suppose sans facteur carré, on peut donc écrire*

$$P = \prod_{i=1}^{r} P_i.$$

Si P n'est pas irréductible, on peut trouver V, non congru à une constante $\bmod P$ *tel que*

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

Lemme 2. *Soit q comme dans le théorème et $R \in \mathbb{F}_q[X]$. L'application*

$$\begin{array}{rccc} S_R : & \mathbb{F}_q[X]/(R) & \to & \mathbb{F}_q[X]/(R) \\ & Q(X) \bmod R & \mapsto & Q(X^q) \bmod R \end{array}$$

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

Démonstration. Le diagramme suivant est commutatif

$$\begin{array}{ccc} \mathbb{F}_q[X] & \xrightarrow{\delta} & \mathbb{F}_q[X] \\ \downarrow{\scriptstyle \pi} & \searrow & \downarrow{\scriptstyle \pi} \\ \mathbb{F}_q[X]/(R) & \xrightarrow[S_R]{} & \mathbb{F}_q[X]/(R), \end{array}$$

où l'on a $\delta : \mathbb{F}_q[X] \to \mathbb{F}_q[X]$, unique morphisme d'anneaux vérifiant $\delta_{|\mathbb{F}_q} = \mathrm{id}$ et $\delta(X) = X^q$. Pour le montrer il suffit de vérifier que (R) est inclus dans le noyau de la flèche diagonale ce qui est évident puisque $\pi \circ \delta(R) = \pi(R)^q = 0$ (car $\mathrm{Carac}(\mathbb{F}_q) = p$). Finalement,

$$S_R(\pi(Q)) = \pi(\delta(Q)) = \pi(Q)^q,$$

d'où la dernière assertion du lemme. □

Démonstration du théorème. Comme les P_i sont premiers deux à deux, le théorème des restes chinois donne l'isomorphisme de $\mathbb{F}_q$-espaces vectoriels suivant

$$\begin{array}{rccc} \varphi : & \mathbb{F}_q[X]/(P) & \to & \prod_{i=1}^{r} \mathbb{F}_q[X]/(P_i) \\ & Q \bmod P & \mapsto & (Q \bmod P_i)_{1 \le i \le r}. \end{array}$$

En notant $K_i = \mathbb{F}_q[X]/(P_i)$, posons

$$\tilde{S}_P = \varphi \circ S_P \circ \varphi^{-1} : K_1 \times \cdots \times K_r \to K_1 \times \cdots \times K_r,$$

qui n'est autre que l'élévation à la puissance q, terme à terme, dans $K_1 \times \cdots \times K_r$. On a donc

$$\begin{aligned} (x_1, \ldots, x_r) \in \ker(\tilde{S}_P - \mathrm{id}) &\iff (x_1^q, \ldots, x_r^q) = (x_1, \ldots, x_r) \\ &\iff \forall i \in \{1, \ldots, r\} \quad x_i^q = x_i \in K_i. \end{aligned}$$

Or, pour une extension quelconque K de $\mathbb{F}_q$, on a $\mathbb{F}_q \hookrightarrow K$, par $\mathbb{F}_q = \{x \in K : x^q = x\}$. En effet, par le théorème de Lagrange on a $\mathbb{F}_q \subset \{x \in K : x^q = x\}$ et l'inclusion réciproque découle du fait que le polynôme $X^q - X$ a au plus q racines dans K. Finalement,

$$(x_1, \ldots, x_r) \in \ker(\tilde{S}_P - \mathrm{id}) \iff \forall i \in \{1, \ldots, r\} \quad x_i \in \mathbb{F}_q \hookrightarrow K_i,$$

donc $\ker(\tilde{S}_P - \mathrm{id}) \simeq (\mathbb{F}_q)^r$ Comme φ est un isomorphismes de $\mathbb{F}_q$-espaces vectoriels, $\ker(\tilde{S}_P - \mathrm{id}) \simeq \ker(S_p - \mathrm{id})$ et on en déduit

$$\dim\Big(\ker(S_P - \mathrm{id})\Big) = r.$$

Comme P est irréductible, on a $r > 1$ et on peut donc trouver $V \mathbb{F}_q[X]$, non congru à une constante $\bmod P$, tel que $V \bmod P \in \ker(S_P - \mathrm{id})$. En effet, les $\alpha \bmod P$, pour $\alpha \in \mathbb{F}_q \hookrightarrow \mathbb{F}_q[X]$, forment un sous-espace vectoriel de dimension 1 de $\mathbb{F}_q[X]/(P)$, engendré par $1 \bmod P$. On note $\alpha_i = V \bmod P_i$ qui vérifie $\alpha_i \in \mathbb{F}_q[X] \hookrightarrow K_i$ puisque $V \bmod P \in \ker(S_P - \mathrm{id})$. Pour $\alpha \in \mathbb{F}_q$, montrons l'égalité

$$P \wedge (V - \alpha) = \prod_{i,\ \alpha_i = \alpha} P_i.$$

Comme $P \wedge (V - \alpha)$ divise P, il est de la forme

$$P \wedge (V - \alpha) = \prod_{i \in I_\alpha} P_i,$$

avec $I_\alpha \subset \{1, \ldots, r\}$. Mais puisque les P_i sont premiers entre eux $I_\alpha = \{i \in \{1, \ldots, r\} : P_i | V - \alpha\}$. Or, pour $i \in \{1, \ldots, r\}$

$$\alpha_i = \alpha \iff V - \alpha = 0 \bmod P_i \iff P_i | V - \alpha,$$

et l'égalité est établie. Finalement,

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

□

Remarque 3. *On est bien présence d'un algorithme de factorisation car* $V - \alpha \neq 0 \bmod P$*, donc* $P \wedge (V - \alpha) \neq P$*. Il y a donc au moins deux facteurs non triviaux dans cette factorisation, qui sont donc de degré inférieur à* P*, et sans facteur carré puisque divisant* P*, on peut donc les factoriser de la même manière.*

I Références

1. Objectif Agrégation, Beck, Malick, Peyré (page 245).