Algorithme de Berlekamp

Benjamin Hellouin

Étant donné P un polynôme unitaire de $\mathbb{F}_p$ avec p premier, on cherche à le décomposer en produit de facteurs premiers irréductibles. Pour l'instant, on suppose que P est sans facteur carré, i.e. $P = P_1 \dots P_r$ deux à deux distincts. On a alors le lemme suivant :

Lemme 1. *Pour tout polynôme Q non constant tel que $Q^p = Q$ dans $\mathbb{F}_p/(P)$, on a $P = \prod_{\alpha \in \mathbb{F}_p} pgcd(P, Q - \alpha)$.*

Preuve. Par le lemme chinois des restes, on a un isomorphisme $\frac{\mathbb{F}_p}{(P)} = \frac{\mathbb{F}_p}{(P_1)} \times \dots \times \frac{\mathbb{F}_p}{(P_r)}$. Si on note $Q \mapsto (Q_1, \dots, Q_r)$ pour l'isomorphisme précédent, $Q = Q^p$ dans $\mathbb{F}_p/(P)$ correspond exactement à $\forall i, Q_i^p = Q_i$ dans $\mathbb{F}_p/(P_i)$.

Comme les P_i sont irréductibles, les (P_i) sont premiers et les $\mathbb{F}_p/(P_i)$ sont des corps sur lesquels le polynôme $X^p - X$ admet au plus p racines. Dans chaque cas, il s'agit exactement des p constantes. Par conséquent, $Q_i \in \mathbb{F}_p$.

Donc $P_i | (Q - \alpha) \Leftrightarrow \alpha = Q_i$ puisque P_i et Q sont non constants,

$$pgcd(P, Q - \alpha) = \prod_{i : Q_i = \alpha} P_i$$

d'où le lemme.

Les pgcd pouvant être calculés efficacement par l'algorithme d'Euclide, on s'intéresse donc à l'équation $Q^p = Q$ qui admet p^r solutions (les r-uplets de constantes). Or le morphisme $\phi : Q \mapsto Q^p$ est linéaire dans $\mathbb{F}_p$, ce qui nous permet de l'écrire sous forme matricielle dans la base $(1, X \dots, X^{n-1})$ où $n = deg(P)$. D'après le nombre de solutions, on aura $\dim \ker(\phi - Id) = r$.

On ne suppose plus que P est sans facteur carré et on va utiliser ces résultats dans l'algorithme suivant :

Algorithme de Berlekamp :

Initialisation : On calcule $D = pgcd(P, P')$. Alors $\frac{P}{D}$ est sans facteur carré, et si $D \neq 1$, on lui applique l'algorithme.

Premier pas : On résout le système $(\phi - Id)(Q) = 0$ pour déterminer r.

Deuxième pas : Si $r = 1$, P est irréductible et on a fini. Si $r \geq 2$, on prend une solution non constante quelconque Q, et le lemme nous fournit une décomposition non triviale $\prod_{\alpha \in \mathbb{F}_p} pgcd(P, Q - \alpha)$.