Algorithme de Berlekamp

Leçons : 122, 123, 125, 141, 151

Réf. : Beck, Objectif intégration p 244

Prop. :

Soit $q = p^\Delta$ où p premier et $\Delta \geq 1$.

Soit $P \in \mathbb{F}_q[X]$ de degré $n \geq 1$ et sans facteur carré.

Alors, on peut déterminer $V \in \mathbb{F}_q[X]$ tel que :

i) V est non constant modulo P

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

iii) si P n'est pas irréductible, au moins deux des facteurs du produit précédent sont non triviaux.

Lemme :

$$S_p : \mathbb{F}_q[X]/(P) \longrightarrow \mathbb{F}_q[X]/(P), \quad y \longmapsto y^q$$

est un morphisme de $\mathbb{F}_q$-algèbres

Lemme :

1) Morphisme d'anneaux

- S_p est bien défini
- $S_p(1) = 1^q = 1$
- $S_p(y+y') = (y+y')^q$

$\mathbb{F}_q$ est de caractéristique p donc

$$(y+y')^p = y^p + y'^p + \sum_{k=1}^{p-1} \underbrace{\binom{p}{k}}_{p\,|\,} y^k y'^{p-k}$$

$$(y+y')^p = y^p + y'^p$$

(idem morphisme de Frobenius)

On a $q = p^n$ donc par récurrence immédiate, $\boxed{S_p(y+y') = S_p(y) + S_p(y')}$

- $S_p(yy') = (yy')^q = y^q y'^q$ car $\mathbb{F}_q[X]/(P)$ est un anneau commutatif

  donc $\boxed{S_p(yy') = S_p(y) S_p(y')}$

$\boxed{S_p \text{ est bien un morphisme d'anneaux}}$

2) Morphisme de $\mathbb{F}_q$-algèbres

$\lambda \in \mathbb{F}_q$.

Si $\lambda = 0$, $\lambda^q = 0 = \lambda$

Si $\lambda \neq 0$, $\lambda \in \mathbb{F}_q^*$ qui est cyclique d'ordre $q-1$

donc $\lambda^{q-1} = 1$

donc $\lambda^q = \lambda$.

Si $y \in \mathbb{F}_q[X]/(P)$, on a $S_p(\lambda y) = \lambda^q y^q = \lambda y^q$

$$\boxed{S_p(\lambda y) = \lambda S_p(y)}$$

donc $\boxed{S_p \text{ est bien un morphisme de } \mathbb{F}_q\text{-algèbres.}}$

Proposition

Notations :

- $P \in \mathbb{F}_q[X]$. On pose $L = \mathbb{F}_q[X]/(P)$ $\mathbb{F}_q$-algèbre de dimension n.
  Soit $\pi : \mathbb{F}_q[X] \longrightarrow L$ la projection canonique, $x = \pi(X)$
  et $\mathcal{B} = (1, x, \dots, x^{n-1})$ une base de L (en tant que $\mathbb{F}_q$-ev)

- On pose $P = \prod_{i=1}^{r} P_i$ la décomposition de P en produit de facteurs irréductibles, tous distincts car P est supposé sans facteur carré.

- Pour $1 \leq i \leq r$, on pose $K_i = \mathbb{F}_q[X]/(P_i)$.
  K_i est alors un corps et $\mathbb{F}_q \subset K_i$

• Enfin, par le théorème des restes chinois,

$$\varphi : L \longrightarrow K_1 \times \dots \times K_r$$
$$\overline{Q} = Q \bmod P \longmapsto (Q \bmod P_1, \dots, Q \bmod P_r)$$

est un isomorphisme de $\mathbb{F}_q$-algèbres.

1) On écrit $\mathrm{Mat}_{\mathcal{B}}(S_p - id)$ et on détermine $\mathrm{rg}(S_p - id)$ par exemple par le pivot de Gauss.

2) $\Pi_q\, r = \dim(\mathrm{Ker}(S_p - id)) = r - \mathrm{rg}(S_p - id)$

• Soit $\tilde{S}_p = \varphi \circ S_p \circ \varphi^{-1}$ (bien défini...)

$$\tilde{S}_p : K_1 \times \dots \times K_r \longrightarrow K_1 \times \dots \times K_r$$
$$(x_1, \dots, x_r) \longmapsto (x_1^q, \dots, x_r^q)$$

$(x_1 \dots x_r) \in \mathrm{Ker}(\tilde{S}_p - id) \iff \forall\, 1 \le i \le r,\ x_i^q = x_i$.

On a : $\forall \alpha \in \mathbb{F}_q \subset K_i,\ \alpha^q = \alpha$ (voir lemme 2)

$\forall x \in K_i$, si $x^q = x$ alors x est racine de $X^q - X \in K_i[X]$ qui admet au plus q racines, dont les éléments de $\mathbb{F}_q$, donc $x \in \mathbb{F}_q$.

On a donc

$$(x_1 \dots x_r) \in \mathrm{Ker}(\tilde{S}_p - id) \iff \forall\, 1 \le i \le r,\ x_i \in \mathbb{F}_q$$

donc $\mathrm{Ker}(\tilde{S}_p - id) \simeq \mathbb{F}_q^r$ et $\dim \mathrm{Ker}(\tilde{S}_p - id) = r$

• $\mathrm{Ker}(\tilde{S}_p - id) = \mathrm{Ker}(\varphi \circ (S_p - id) \circ \varphi) = \varphi(\mathrm{Ker}(S_p - id))$ et φ est un isomorphisme,

donc $\dim \mathrm{Ker}(S_p - id) = r$.

Rq : Si $r = 1$, on s'arrête là et P est irréductible.

2) Si $n > 1$. Montrer le i) et ii) de la proposition

a°/ Soit $\mathcal{D} = \{ \overline{V} \in L$, V constant modulo $P \}$

$= \{ \overline{V} \in L \quad / \exists \alpha \in \mathbb{F}_q, \ \overline{V} = \overline{\alpha} \}$

$= \{ \overline{V} \in L \quad / \exists \alpha \in \mathbb{F}_q, \ \overline{V} = \alpha . \overline{1} \}$

$\mathcal{D} = Vect(\overline{1})$

$\dim \mathcal{D} = 1$ et $\dim(Ker(S_p - id)) = n > 1$ donc

$\exists V \in \mathbb{F}_q[X] \ / \ \overline{V} \in Ker(S_p - id)$ et $\overline{V} \notin \mathcal{D}$

On pose alors

$\varphi(\overline{V}) = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}_q^n$ car $\overline{V} \in Ker(S_p - id)$

b°/ Soit $\alpha \in \mathbb{F}_q$. Π_q $Q_\alpha = pgcd(P, V - \alpha) = \prod_{\substack{1 \le i \le n \\ \alpha_i = \alpha}} P_i$

. $Q_\alpha \mid P$ et $P = \prod_{i=1}^{n} P_i$ donc il existe $I_\alpha \subset \{1 \dots n\}$ tel que $Q_\alpha = \prod_{i \in I_\alpha} P_i$ (unicité de la décomposition en facteurs irréductibles)

. $Q_\alpha \mid V - \alpha$ donc par le lemme de Gauss, $P_i \mid V - \alpha$ $\forall i \in I_\alpha$

donc $I_\alpha = \{ 1 \le i \le n, \ V = \alpha \bmod P_i \}$

$I_\alpha = \{ 1 \le i \le n, \ \alpha_i = \alpha \}$

donc $Q_\alpha = pgcd(P, V - \alpha) = \prod_{\substack{1 \le i \le n \\ \alpha_i = \alpha}} P_i$

c°/ Enfin, $\{1 \dots n\} = \coprod_{\alpha \in \mathbb{F}_q} I_\alpha$

donc $P = \prod_{i=1}^{n} P_i = \prod_{\alpha \in \mathbb{F}_q} \left(\prod_{i \in I_\alpha} P_i \right)$

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

(6)

3) Montrer le iii), et donc que l'algorithme s'arrête.

Par construction $\overline{V} \notin \mathcal{D} = \mathrm{Vect}(\bar{1})$

donc $\varphi(\overline{V}) = (\alpha_1 \dots \alpha_n) \neq (\alpha, \dots, \alpha)$

car φ est un isomorphisme.

Par conséquent,

il existe $1 \leq i, j \leq n$, $i \neq j$ tels que $\alpha_i \neq \alpha_j$

donc au moins deux facteurs du produit dans $(*)$ sont non triviaux.

On recommence alors à l'étape 1) pour ces facteurs non triviaux.