réf : [BMP] pp. 245-247 et 251
[Ber]
[Berm] pp. 232-233

leçons :
122
123
141
142
151
125

Algorithme de Berlekamp

Soit $P \in \mathbb{F}_q[X]$ sans facteur multiple.

Alors $E = \mathbb{F}_q[X]/(P)$ est une $\mathbb{F}_q$-algèbre, $u : E \to E$, $Q \mapsto Q^q$ est un endomorphisme de E

(i) et $r := \dim \ker (u - id)$ est le nombre de facteurs irréductibles de P dans $\mathbb{F}_q[X]$.

De plus, si $V \in \mathbb{F}_q[X]$ vérifie : (et si $r > 1$)
$\begin{cases} V \text{ non congru à un polynôme constant modulo } P \\ V \bmod P \in \ker(u - id) \end{cases}$

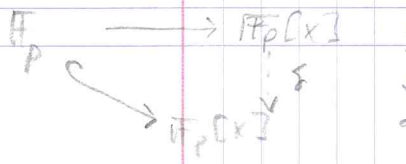
(ii) alors : $\boxed{P = \prod_{\alpha \in \mathbb{F}_q} P \wedge (V - \alpha)}$

Écrivons $P = \prod_{i=1}^{r} P_i$ où les P_i sont irréductibles et premiers entre eux.

(1) $E = \mathbb{F}_q[X]/(P)$ est un anneau, qui hérite de la structure de $\mathbb{F}_q$-ev de $\mathbb{F}_q[X]$.

(2) Linéarité de u

Par la propriété universelle des polynômes, $\exists!$ m d'a $\delta : \begin{cases} \mathbb{F}_q[X] \to \mathbb{F}_q[X] \\ a \in \mathbb{F}_q \mapsto a \\ X \mapsto X^q \end{cases}$



Mais pour tout $Q \in \mathbb{F}_q[X]$,

$$\delta(Q) = Q(X^q) = Q(X)^q$$

car la caractéristique de $\mathbb{F}_q[X]$ divise q, et car dans $\mathbb{F}_q$: $a^q = a$.

$(Q+P)^q = Q^q + P^q$

$(\sum a_i X^i)^q = \sum (a_i X^i)^q = \sum a_i X^{iq}$

Donc on a

$$\begin{array}{ccccc} \mathbb{F}_q[X] & \xrightarrow{\delta} & \mathbb{F}_q[X] & \xrightarrow{\pi} & \mathbb{F}_q[X] \\ & & \pi \downarrow & \nearrow u & \\ & & \mathbb{F}_q[X]/(P) & & \end{array}$$

où $\pi \circ \delta$ se factorise car :

$$\pi \circ \delta(P) = \overline{P^q} = \overline{P}^q = \overline{0}$$

et on vérifie, si $\overline{Q} \in \mathbb{F}_q[X]/(P)$:

$$u(\overline{Q}) = \overline{Q^q} = \overline{Q}^q$$

et u hérite de la linéarité de δ.

(3) $E = \mathbb{F}_q[X]/(P)$ est $\mathbb{F}_q$-isomorphe à $\prod_{i=1}^{\hat{r}} \mathbb{F}_{q^{d_i}}$

$(P_i)_i$ premiers entre eux $\Rightarrow$ $(P_i)_i$ idéaux étrangers

donc le théorème chinois donne un isomorphisme d'anneaux,

$$\varphi : \mathbb{F}_q[X]/(P) \longrightarrow \prod_{i=1}^{\hat{r}} \mathbb{F}_q[X]/(P_i)$$

et comme chaque P_i est irréductible, $\mathbb{F}_q[X]/(P_i)$ est un corps à q^{d_i} éléments que l'on peut noter $\mathbb{F}_{q^{d_i}}$ (car unique à isom. près).

(4) $\ker(u - id)$ est $\mathbb{F}_q$-isomorphe à $\mathbb{F}_q^r$

Comme φ est un isomorphisme, on a :

si $x = (x_1, \dots, x_n) \in \prod \mathbb{F}_{q^{d_i}}$:

$y := \varphi^{-1}(x) \in \ker(u - id) \iff y^q = y$

$\iff x^q = x$

$\iff x_i^q = x_i \quad \forall i$

or dans chaque $\mathbb{F}_{q^{d_i}}$, l'ensemble

$\{ x \in \mathbb{F}_{q^{d_i}} \mid x^q = x \}$ *

forment l'unique sous-corps de $\mathbb{F}_{q^{d_i}}$ à q éléments que l'on peut noter $\mathbb{F}_q$ (abusivement car tous isomorphes). On conclut donc :

$$\ker(u - id) \simeq \mathbb{F}_q{}^n$$

et $\underline{n = \dim_{\mathbb{F}_q} \ker(u - id)} = d^\circ P - \operatorname{rg}(u - id)$

(5) Contentons (i.i). Si $n \geq 1$, comme $\{ \overline{U} \in E \mid U \equiv \alpha \bmod P, \alpha \in \mathbb{F}_q \} = \mathbb{F}_q \cdot 1_E$ est une droite, il existe $\overline{V} \in \ker(u - id)$ tel que $V \bmod P$ n'est pas constant.

On note : $\overline{V} \in \ker(u - id) \Rightarrow \alpha_i := V \bmod P_i \in \mathbb{F}_q$ (P_i)

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

$D_\alpha \mid P = \prod_{i=1}^{r} P_i$

donc $D_\alpha = \prod_{j \in J_\alpha^c} P_j$ où $J_\alpha \in [\![1, n]\!]$

or comme $\begin{cases} D_\alpha \mid V - \alpha \\ (P_j)_{j \in J_\alpha} \text{ premiers entre eux,} \end{cases}$

alors $\forall j \in J_\alpha, \ P_j \mid V - \alpha$

par le lemme de Gauss,

* c'est un sous-corps, donc de cardinal $\in \{1, p, p^2, \dots, p^{d_i}\}$ donc $= q$

donc $J_\alpha = \{ j \in [\![1,n]\!] \mid P_j \mid V - \alpha \}$

$= \{ j \in [\![1,n]\!] \mid V = \alpha \mod P_i \}$

$= \{ j \in [\![1,n]\!] \mid \alpha_i = \alpha \}$ $\quad \alpha \in \mathbb{F}_q$

donc $D_\alpha = \prod_{\{j,\ d_j = d_j\}} P_j$

et $P = \prod_{i=1}^{n} P_i = \prod_{\alpha \in \mathbb{F}_q} \prod_{\{j,\ d_j = \alpha_j\}} P_j = \prod_{\alpha \in \mathbb{F}_q} P \wedge (V - \alpha)$.

En pratique **Algorithme :**

- Dans la base $\mathcal{B} = (\bar{1}, \bar{X}, \dots, \bar{X}^{d^\circ P - 1})$ on calcule la matrice $M = \mathrm{Mat}_{\mathcal{B}} u$

avec $u(\bar{X}^k) = \overline{X^{qk}} = \sum_{i=0}^{d^\circ P - 1} a_{k,i} \bar{X}^i$

↳ division euclidienne par P

(ce qui donne $M = (a_{k,i})_{0 \leq k,i \leq d^\circ P - 1}$)

et on calcule $\mathrm{rg}(M - I)$ grâce au pivot de Gauss.

- Si $n = 1$: on s'arrête, sinon :

On calcule V, et les $P \wedge (V - \alpha)$ grâce à Euclide.

Comme on a pris V non congru à une constante mod P,

$\exists\ \alpha_i \neq \alpha_j \in \mathbb{F}_p$, $V \equiv \alpha_i\ [P_i]$ et $V \equiv \alpha_j\ [P_j]$

donc $P \wedge (V - \alpha_i)$ et $P \wedge (V - \alpha_j)$ sont non triviaux ($\neq P, 1$)

donc les $P \wedge (V - \alpha)$ ont $< n$ facteurs irréd

Donc on recommence avec ces facteurs, et l'algorithme se termine. (qui sont sans facteur mu- tt.)