L'oral à l'agreg - Isenmann

Algorithme de Berlekamp

120 125
121 141
122 142
123 151

Proposition : $S : \begin{array}{ccc} \mathbb{F}_q[X] & \to & \mathbb{F}_q[X] \\ Q & \mapsto & Q^q \end{array}$ est un $\mathbb{F}_q$-endomorphisme de l'ev $\mathbb{F}_q[X]$.

Preuve :

* $S(\lambda R) = \lambda S(R)$ (car $\lambda^q = \lambda$ dans $\mathbb{F}_q$)
* $\mathbb{F}_q$ est de caractéristique p et alors $(Q+R)^p = Q^p + R^p$
  Puis, par récurrence, $(Q+R)^{p^k} = Q^{p^k} + R^{p^k}$
  En particulier : $S(Q+R) = S(Q) + S(R)$.

Ainsi, S est $\mathbb{F}_q$-linéaire.

Lemme : Soit $\mathbb{L}$ une extension de $\mathbb{F}_q$ et $x \in \mathbb{L}$.
Alors : $x^q = x$ ssi $x \in \mathbb{F}_q$

Preuve :
Pour tout $x \in \mathbb{F}_q^*$, $x^{q-1} = 1$.
Ainsi, pour tout $\mathbb{F}_q \ni x$, $x^q = x$.
On a exhibé q racines distinctes du polynôme $P = X^q - X$ sur $\mathbb{L}$.
Or : $\mathbb{L}$ est un corps et P est de degré q donc P possède au plus q racines.

Théorème : (des restes chinois)
Soit $(P_1; \dots; P_r) \in \mathbb{F}_q[X]^r$ polynômes premiers entre eux et $P = \prod_{i=1}^{r} P_i$.
Alors : $\begin{array}{ccc} \mathbb{F}_q[X]/\langle P\rangle & \to & \mathbb{F}_q[X]/\langle P_1\rangle \times \dots \times \mathbb{F}_q[X]/\langle P_r\rangle \\ Q \bmod(P) & \mapsto & (Q \bmod(P_1); \dots; Q \bmod(P_r)) \end{array}$
est un isomorphisme de $\mathbb{F}_q$-algèbres.

Théorème : Soit $q = p^n$ avec p premier, $n \in \mathbb{N}$, $P \in \mathbb{F}_q[X]$ sans facteur carré et $P = \prod_{i=1}^{r} P_i$ la décomposition de P en produit d'irréductibles sur $\mathbb{F}_q[X]$.
Alors : (1) Si $r = 1$, alors P est irréductible
(2) Sinon, il existe $a \in \mathbb{F}_q$ et $V \in \mathbb{F}_q[X]$ tq : $PGCD(P; V-a)$ est facteur non-trivial de P

Preuve :
Soit $T : \begin{array}{ccc} \mathbb{F}_q[X] & \to & \mathbb{F}_q[X]/\langle P\rangle \\ Q & \mapsto & Q^q \bmod(P) \end{array}$ morphisme $\mathbb{F}_q$-linéaire par composition de l'application $\begin{array}{ccc} \mathbb{F}_q[X] & \to & \mathbb{F}_q[X] \\ Q & \mapsto & Q^q \end{array}$ par la surjection canonique qui sont eux-mêmes $\mathbb{F}_q$-linéaires.

Par ailleurs, pour tout $Q \in \mathbb{F}_q[X]$, $T(QP) = 0$ donc $\langle P\rangle \subseteq \ker(T)$

On peut alors factoriser T en un $\mathbb{F}_q$-endomorphisme
$\varphi : \begin{array}{ccc} \mathbb{F}_q[X]/\langle P\rangle & \to & \mathbb{F}_q[X]/\langle P\rangle \\ Q & \mapsto & Q^q \end{array}$

Soit $K = \mathbb{F}_q[X]/\langle P\rangle$ et pour tout $i \in [\![1; r]\!]$, $K_i = \mathbb{F}_q[X]/\langle P_i\rangle$.
Par le théorème des restes chinois, il existe un isomorphisme $\psi : K \to K_1 \times \dots \times K_r$ de $\mathbb{F}_q$-algèbres.
Soit $\tilde{\varphi} = \psi \circ \varphi \circ \psi^{-1}$

$$\begin{tikzcd} K_1 \times \dots \times K_r \arrow[d, "\psi^{-1}"'] & K \arrow[l, "\psi"'] \\ K \arrow[ur, "\varphi"'] & \end{tikzcd}$$

Ainsi, pour tout $(Q_1; \dots; Q_r) \in K_1 \times \dots \times K_r$, $\tilde{\varphi}(Q_1; \dots; Q_r) = (Q_1^q; \dots; Q_r^q)$ et alors pour tout $i \in [\![1; r]\!]$, $Q_i^q = Q_i$ ssi $(Q_1; \dots; Q_r) \in \ker(\tilde{\varphi} - id)$.
Or : pour tout $i \in [\![1; r]\!]$, K_i est une extension de $\mathbb{F}_q$.
Par le lemme, $Q_i^q = Q_i$ ssi $Q_i \in \mathbb{F}_q$
Alors : $\#\ker(\tilde{\varphi} - id) = q^r$
Ainsi, $\dim(\ker(\tilde{\varphi} - id)) = \dim(\ker(\varphi - id)) = r$.

Puisque le cas $r = 1$ est immédiat, supposons $r \geq 2$.
Ainsi, puisque les polynômes constants modulo P forment un sous-ev de K de dimension 1 engendré par 1 et puisque $\dim(\ker(\varphi - id)) \geq 2$, il existe $V \in \mathbb{F}_q[X]$ non-constant modulo P tel que $V^q = V \bmod(P)$.
Soit un tel polynôme V.
En particulier, pour tout $i \in [\![1; r]\!]$, $V^q = \alpha_i := V \bmod(P_i)$
Par le lemme, pour tout $i \in [\![1; r]\!]$, $\alpha_i \in \mathbb{F}_q$.

Montrons qu'il existe $i, j \in [\![1; r]\!]$ tels que $\alpha_i \neq \alpha_j$.
Supposons par l'absurde que pour tout $i, j \in [\![1; r]\!]$, $\alpha_i = \alpha_j$.
Ainsi, il existe $\alpha \in \mathbb{F}_q$ tel que pour tout $i \in [\![1; r]\!]$, $V = \alpha \bmod(P_i)$
Par injectivité de ψ, $V = \alpha \bmod(P)$.
ABSURDE puisque on a supposé V non-constant modulo P.

Soit de tels i et j, et soit $Q = PGCD(P; V - \alpha_i)$.

* $P_i \mid P$ et $P_i \mid V - \alpha_i$ (car $V = \alpha_i \bmod(P_i)$) donc $P_i \mid Q$
* $P_j \nmid V - \alpha_i$ (car $\alpha_i \neq \alpha_j$) donc $P_j \nmid Q$

On a alors fabriqué Q diviseur non-trivial de P.

Temps

16,33

Temps
22'46''