[Obj. Agreg, Beck] 244

Algorithme de Berlekamp :

Leçons 123 141 151 (125) (122) (142) ((121))

Soit p premier, $n \in \mathbb{N}^*$, $q = p^n$.

L'algorithme de Berlekamp prend en paramètre un polynôme $P \in \mathbb{F}_q[X]$ sans facteur carré (i.e. $\nexists Q$ tq $Q^2 | P$, i.e. $P \wedge P' = 1$) et renvoie l'union de ses facteurs irréductibles.

Lemme : Soit $R \in \mathbb{F}_q[X]$. L'application $S_R : \dfrac{\mathbb{F}_q[X]}{(R)} \longrightarrow \dfrac{\mathbb{F}_q[X]}{(R)}$, $\overline{Q(X)} \longmapsto \overline{Q(X^q)}$ est bien définie et coïncide avec l'élévation à la puissance q dans $\dfrac{\mathbb{F}_q[X]}{(R)}$.

[Beck 245]

Preuve :

Soit $S_1 : \mathbb{F}_q[X] \longrightarrow \mathbb{F}_q[X]$, $Q(X) \longmapsto Q(X^q)$ qui est un morphisme d'anneau (prop univ des polynômes) correspondant à l'élévation à la puissance q.

On note $\pi : \mathbb{F}_q[X] \longrightarrow \dfrac{\mathbb{F}_q[X]}{(R)}$ la surjection canonique et on note $S = \pi \circ S_1 : \mathbb{F}_q[X] \longrightarrow \dfrac{\mathbb{F}_q[X]}{(R)}$. Le morphisme S (car composée de morphisme) passe au quotient par (R) (car $S(R) = \pi \circ S_1(R) = \pi(R(X^q)) \underset{\text{dans } \mathbb{F}_q,\ a^q = a}{=} \pi(R^q) = \pi(R)^q = 0$)

et donne S_R qui est donc bien définie.

Soit $Q \in \mathbb{F}_q[X]$. $S_R(Q \bmod (R)) = S_R(\pi(Q)) \underset{\text{def de } S_R}{=} \pi(Q(X^q)) \underset{a \in \mathbb{F}_q \Rightarrow a^q = a}{=} \pi(Q^q)$

$= \pi(Q)^q$ ∎

Algorithme de Berlekamp : [Beck 245]

Soit $P \in \mathbb{F}_q[X]$ sans facteurs carrés. On note $\pi : \mathbb{F}_q[X] \longrightarrow \dfrac{\mathbb{F}_q[X]}{(P)}$ la proj canonique et $x = \pi(X)$. On considère $\{1, x, \dots, x^{\deg(P-1)}\}$ de $\dfrac{\mathbb{F}_q[X]}{(P)}$.

Le processus suivant s'arrête après un nombre fini d'étape et renvoie l'union des facteurs irréductibles de P.

① On calcule M la matrice de $S_p - Id$ dans la base $\mathcal{B}$.

② Le nbre de facteurs irréductibles de P est $r = \dim \ker(S_p - Id)$.
$= \deg(P) - rg(S_p - Id)$

si $r = 1$, on renvoie P qui est irréductible et on arrête l'algo.
Sinon, on passe à l'étape suivante.

③ On calcule un polynôme υ non congru à un polynôme constant de $\mathbb{F}_q[X]$ modulo P et tel que $\upsilon \bmod P \in \ker(S_p - Id)$.
Avec l'algorithme d'Euclide, on calcule ensuite les pgcd $(P, \upsilon - \alpha)$. On a alors :

$$P = \prod_{\alpha \in \mathbb{F}_q} \operatorname{pgcd}(P, \upsilon - \alpha)$$

On retourne en ① avec chacun des facteurs non triviaux de ce produit.

Preuve :

▶ Mq $r = \dim(\ker(S_p - Id))$

Soit $P = P_1 \times \dots \times P_r$ la décomposition en produit d'irréductibles deux à deux distincts de P.

$\forall i \in [\![1, r]\!]$, on pose $K_i = \dfrac{\mathbb{F}_q[X]}{(P_i)}$. Le théorème chinois fournit l'isomorphisme de $\mathbb{F}_q$-algèbres

$$\varphi : \frac{\mathbb{F}_q[X]}{(P)} \longrightarrow K_1 \times \dots \times K_r$$
$$\overline{Q}^P \longmapsto \left(\overline{Q}^{P_1}, \dots, \overline{Q}^{P_r}\right)$$

i.e. $Q \bmod P_r$

On pose alors $\tilde{S}_p = \varphi \circ S_p \circ \varphi^{-1}$ qui correspond à l'élévation à la puissance q composante par composante dans l'anneau $K_1 \times \dots \times K_r$.

Alors $(x_1, \dots, x_r) \in \ker(\tilde{S}_p - Id) \Leftrightarrow (x_1^q, \dots, x_r^q) = (x_1, \dots, x_r)$
$\Leftrightarrow \forall i \in [\![1, r]\!],\ x_i^q = x_i$ dans K_i.

Soit $\mathbb{K}$ une extension de corps de $\mathbb{F}_q$. Alors l'image de $\mathbb{F}_q$ dans $\mathbb{K}$ est l'ensemble des éléments de $\mathbb{K}$ tq $x^q = x$. (en effet : si $x \in \mathbb{F}_q^\times$, par le thm de Lagrange, $x^{q-1} = 1$ donc $x^q = x$. 0 vérifie aussi cette égalité, elle est donc vraie $\forall x \in \mathbb{F}_q$. De plus, $X^q - X \in \mathbb{K}[X]$ est de degré q et dispose déjà de q racines, il n'y a donc pas d'autres éléments de $\mathbb{K}$ vérifiant $X^q = X$. Ainsi l'image de $\mathbb{F}_q$ dans $\mathbb{K}$ est l'ensemble des éléments de $\mathbb{K}$ vérifiant $x^q = x$).

donc $(x_1, \dots, x_n) \in \ker(\tilde{S}_P - Id) \iff \forall i \in [\![1,n]\!],\ x_i \in \mathbb{F}_q$. Ainsi

$\ker(\tilde{S}_P - Id) \simeq \mathbb{F}_q^n$ donc $n = \dim(\ker(\tilde{S}_P - Id))$. Or

φ isomorphisme de $\mathbb{F}_q$ ev et $\ker(\tilde{S}_P - Id) = \varphi(\ker(S_P - Id))$

donc $\dim(\ker(S_P - Id)) = n$.

▶ On mq on peut trouver un tel υ (pour $n > 1$)

Supposons $n > 1$.

Remarquons que l'ensemble des $(\upsilon \bmod P)$ où υ est congru à un polynôme constant modulo P et la droite vectorielle de $\frac{\mathbb{F}_q[X]}{(P)}$ engendrée par 1.

Or, $n = \dim \ker(S_P - Id) > 1$ donc $\exists\, \upsilon \in \mathbb{F}_q[X]$ non congru modulo P à un polynôme constant tq $(\upsilon \bmod P) \in \ker(S_P - Id)$.

▶ Montrons l'égalité

$(\upsilon \bmod P) \in \ker(S_P - Id) \iff (\upsilon \bmod P_1, \dots, \upsilon \bmod P_n) \in (\mathbb{F}_q)^n$.

$\forall i \in [\![1, \dots, n]\!]$, on note $\alpha_i = (\upsilon \bmod P_i) \in \mathbb{F}_q \subset K_i$.

$\forall \alpha \in \mathbb{F}_q$, montrons que $\text{pgcd}(P, \upsilon - \alpha) = \prod_{\{i\,;\,\alpha_i = \alpha\}} P_i$

Comme $\text{pgcd}(P, \upsilon - \alpha) \mid P$, on a $\text{pgcd}(P, \upsilon - \alpha) = \prod_{i \in I_\alpha} P_i$ avec $I_\alpha \subset [\![1,n]\!]$

Or, les P_i sont deux à deux premiers entre eux. Par le lemme de Gauss,

$I_\alpha = \{ i \in [\![1,n]\!] ;\ P_i \mid \upsilon - \alpha \}$.

Mais $\forall i \in [\![1,n]\!]$, on a :

$\alpha_i = \alpha \Leftrightarrow \sigma - \alpha = 0 \mod P_i \Leftrightarrow P_i \mid \sigma - \alpha$

donc $I_\alpha = \{ i \in [\![1,n]\!] ; \alpha_i = \alpha \}$ et ainsi $\operatorname{pgcd}(P, \sigma - \alpha) = \prod_{\{i ; \alpha_i = \alpha\}} P_i$.

On a alors
$$P = \prod_{i=1}^{n} P_i = \prod_{\alpha \in \mathbb{F}_q} \left(\prod_{\{i ; \alpha_i = \alpha\}} P_i \right)$$
$$= \prod_{\alpha \in \mathbb{F}_q} \operatorname{pgcd}(P, \sigma - \alpha). \quad (*)$$

▶ Mq l'algorithme s'arrête :

Mq n diminue à chaque itération :

Le choix d'un σ non congru à un pol constant mod P

assure que $\exists (i,j) \in [\![1,n]\!]^2$ tq $\alpha_i \neq \alpha_j$.

Ainsi, parmi les facteurs apparaissant dans $(*)$, au moins deux sont

non triviaux et donc ont chacun moins de n facteurs irréductibles

(De plus, chaque nouveau polynôme étant un diviseur de P, il est

bien sûr sans facteur carré).

<u>Remarque</u> : Et si P a des facteurs carrés ?

<u>Algo de factorisation</u> : Soit $P \in \mathbb{F}_q[X]$.

① Si P constant, arrêter l'algo

② On calcul $U = \operatorname{pgcd}(P, P')$.

Si $U = 1$: Appliquer l'algo de Berlekamp à P

Si $U = P$: On calcul R tq $R^p = P$ et on retourne en 1 avec R

Sinon : soit $\sigma = \frac{P}{U}$. On retourne en ① avec U et σ.

Question (sur der Algo de Berlekamp)

Q1: Coût de l'algo ?

↳ pour P de degré n, sur $\mathbb{F}_q[X]$, coût $= \mathcal{O}(q\, n^3)$

Q2: Comment calculer $M = S_{\mathbb{K}} - Id$?

↳ Exprimer $S(\{X_i\})$ dans $\{X_i\}$

c-à-d les $(X_i)^q$ dans $\{X_i\}$

Q3: Quand a-t-on $\mathbb{F}_q \subset \mathbb{F}_{q'}$?

Quand $x \in \mathbb{F}_q$ et $x^{q'} = x$.

Exercice: (un peu hors sujet)

$\mathbb{K}$ et $\mathbb{L}$ deux extensions tq $\mathbb{K} \subset \mathbb{L}$.

$P, Q \in \mathbb{K}[X]$. On note $D_{\mathbb{K}}$ le pgcd de (P, Q) dans $\mathbb{K}[X]$

$D_{\mathbb{L}}$ ——— $\mathbb{L}[X]$

Est ce la même chose ?

Solution:

- $P \in \mathbb{K}[X] \subset \mathbb{L}[X]$ et $Q \in \mathbb{K}[X] \subset \mathbb{L}[X]$.

  $D_{\mathbb{K}} \mid P$ et $D_{\mathbb{K}} \mid Q$ dans $\mathbb{L}[X]$ donc $D_{\mathbb{K}} \mid D_{\mathbb{L}}$.

- Si $P = P' . D_{\mathbb{L}}$, $Q = Q' . D_{\mathbb{L}}$ dans $\mathbb{L}[X]$.

$$(D_{\mathbb{K}}) = (P)_{\mathbb{K}} + (Q)_{\mathbb{K}}$$
$$\cap \qquad\qquad \cap$$
$$(D_{\mathbb{L}}) = (P)_{\mathbb{L}} + (Q)_{\mathbb{L}}$$

donc $(D_{\mathbb{K}}) \subset (D_{\mathbb{L}})$

donc $D_{\mathbb{L}} \mid D_{\mathbb{K}}$.

---

info: Application : La factorisation dans les corps finis est une étape de la factorisation dans $\mathbb{Z}[X]$. Soit $P \in \mathbb{Z}[X]$. On se ramène dans $\mathbb{F}_q[X]$ en passant modulo q. On calcule les facteurs irréd de P dans $\mathbb{F}_q[X]$. Puis on utilise le principe de remontée de Hensel pour en déduire la factorisation de P sur $\mathbb{F}_{q^2}[X]$ puis sur $\mathbb{F}_{q^4}[X]$ etc... La borne de Landau-Mignotte permet de majorer le nbre de remontée nécessaire, et la factorisation sur $\mathbb{F}_{q^{e}}[X]$ correspond à celle sur $\mathbb{Z}[X]$.

X^4+1 sur $\mathbb{F}_3[X]$: $\quad S_p : \dfrac{\mathbb{F}_3[X]}{(X^4+1)} \longrightarrow \dfrac{\mathbb{F}_3[X]}{(X^4+1)}$

$\qquad\qquad\qquad\qquad\qquad \overline{Q(X)} \longmapsto \overline{Q(X^3)}$

$Sp(1) = 1-1 = 0$

$Sp(X) = X^3 - X$

$Sp(X^2) = X^6 - X^2$
$= -X^2 - X^2$
$= -2X^2$

$Sp(X^3) = X^9 - X^3$
$= X - X^3$

$$M = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -2 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

$$\ker M = \mathrm{Vect}\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \right\}$$

On prend par ex. $v = X^3 + X + 1$

① $\mathrm{pgcd}(X^4+1, X^3+X+1)$:

X^4+1	X^3+X+1	$-X^2-X+1$	$3X = 0$ dans $\mathbb{F}_3$
	X	$-X+1$	

d'où $\mathrm{pgcd}(X^4+1, X^3+X+1) = +X^2+X-1$

(irréductible car de d° 2 et sans racine).

② $\mathrm{pgcd}(X^4+1, X^3+X+1-1) = 1$

③ $\mathrm{pgcd}(X^4+1, X^3+X+1-2) = X^2-X-1$

d'où $X^4+1 = (X^2+X-1)(X^2-X-1)$