Algorithme de Berlekamp

Leçons : 125, 141, 151, 142, (123)
Réf : BMP, Objectif Agreg p245

Soit p un nombre premier, $\mathbb{F}_q$ le corps à $q = p^s$ éléments et $P \in \mathbb{F}_q[X]$ de degré $n \geq 1$ sans facteur carré qu'on écrit $P = P_1 \cdots P_r$ où les P_i sont irréductibles et premiers entre eux 2 à 2.
L'algorithme de Berlekamp calcule le nombre r de facteurs irréductibles de P et lorsque $r \geq 2$, donne exactement les P_i.

Lemme : Si $R \in \mathbb{F}_q[X]$, l'application $S_R : \begin{array}{ccc} \mathbb{F}_q[X]/(R) & \longrightarrow & \mathbb{F}_q[X]/(R) \\ Q(X) \bmod R & \longmapsto & Q(X^q) \bmod R \end{array}$ est bien définie et coïncide avec l'élévation à la puissance q dans $\mathbb{F}_q[X]/(R)$.

Dém : $\varphi : Q(X) \in \mathbb{F}_q[X] \longmapsto Q(X^q) \in \mathbb{F}_q[X]$ est un morphisme d'anneaux qui coïncide avec l'élévation à la puissance q car la caractéristique du corps divise q et car $\forall x \in \mathbb{F}_q$, $x^q = x$. Si $\pi : \mathbb{F}_q[X] \longrightarrow \mathbb{F}_q[X]/(R)$, $\pi \circ \varphi(R) = 0$ donc $\pi \circ \varphi : \mathbb{F}_q[X] \longrightarrow \mathbb{F}_q[X]/(R)$ passe au quotient pour donner S_R, qui est donc bien définie. De plus,

$$S_R(Q \bmod R) = S_R(\pi(Q)) = \pi\circ\varphi(Q) = \pi(Q(X^q)) = \pi(Q^q) = \pi(Q)^q. \square$$

Rmq : S_R est même un morphisme de $\mathbb{F}_q$-algèbre (la $\mathbb{F}_q$-linéarité venant de Frobenius)

On considère les $\mathbb{F}_q$-espaces vectoriels de dim. finie $K_i = \mathbb{F}_q[X]/(P_i)$.
Comme P_i est irréductible, K_i est un corps et le théorème chinois fournit l'isomorphisme de $\mathbb{F}_q$-algèbres $\varphi : \begin{array}{ccc} \mathbb{F}_q[X]/(P) & \longrightarrow & K_1 \times \cdots \times K_r \\ Q \bmod P & \longmapsto & (Q \bmod P_1, \ldots, Q \bmod P_r) \end{array}$

car les P_i sont premiers entre eux 2 à 2.

Prop : On pose $x = X \bmod P$ et on considère la base $\mathcal{B} = (1, x, \ldots, x^{n-1})$ de $\mathbb{F}_q[X]/(P)$.
Alors le processus suivant (algo. de Berlekamp) s'arrête au bout d'un nb. fini d'étapes et donne la décomposition en facteurs irréductibles de P.

i) on calcule la matrice de $S_p - Id$ dans la base $\mathcal{B}$.

ii) le nombre de facteurs irréductibles de P est donné par

$r = \dim(\mathrm{Ker}(S_p - Id)) = \deg P - \mathrm{rg}(S_p - Id)$

Si $r = 1$, on a fini, sinon :

iii) on calcule un polynôme $V \in \mathbb{F}_q[X]$ non constant modulo P et tel que $V \bmod P \in \mathrm{Ker}(S_p - Id)$. Avec l'algorithme d'Euclide, on calcule $\mathrm{pgcd}(P, V-\alpha)$ $\forall \alpha \in \mathbb{F}_q$. On a alors $P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V-\alpha)$ et on répète le processus avec chacun des facteurs non triviaux de ce produit.

Dém : On pose $\tilde{S}_p = \varphi \circ S_p \circ \varphi^{-1} : K_1 \times \cdots \times K_r \longrightarrow K_1 \times \cdots \times K_r$ qui correspond à l'élévation à la puissance q dans $K_1 \times \cdots \times K_r$ (i.e composante par composante). De plus,

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

car $X^q - X$ possède $q = \mathrm{Card}\,\mathbb{F}_q$ racines dans K_i : on les a toutes.

Or comme les P_i sont irréductibles, les K_i sont des extensions finies de $\mathbb{F}_q$ donc on sait par construction des corps finis que les éléments invariants par $x \mapsto x^q$ dans K_i sont exactement les éléments de $\mathbb{F}_q$.

Donc $(x_1, \dots, x_r) \in \mathrm{Ker}(\tilde{S}_p - Id) \iff \forall 1 \leq i \leq r,\ x_i \in \mathbb{F}_q \hookrightarrow K_i$

i.e $\mathrm{Ker}(\tilde{S}_p - Id) \simeq \mathbb{F}_q^r$ donc est de dimension r et comme φ est un iso. de $\mathbb{F}_q$-ev, $\dim(\mathrm{Ker}(S_p - Id)) = \dim(\mathrm{Ker}(\tilde{S}_p - Id)) = r$.

Supposons $r > 1$. Remarquons que $\mathcal{D} = \{U \bmod P : U \text{ constant mod } P\}$

$= \{U \bmod P : \exists \alpha \in \mathbb{F}_q,\ \bar{U} = \alpha \cdot \bar{1}\}$

$= \mathrm{Vect}(1 \bmod P)$ est une droite vectorielle de $\mathbb{F}_q[X]/(P)$. Comme $r = \dim(\mathrm{Ker}(S_p - Id)) > 1$, il existe $V \in \mathbb{F}_q[X]$ non constant mod P et tel que $V \bmod P \in \mathrm{Ker}(S_p - Id)$.

On pose $\varphi(V \bmod P) = (\alpha_1, \dots, \alpha_r) \in \mathbb{F}_q^r$ (car $V \bmod P \in \mathrm{Ker}(S_p - Id)$).

Pour $\alpha \in \mathbb{F}_q$, montrons que $\underbrace{\mathrm{pgcd}(P, V-\alpha)}_{:= Q_\alpha} = \prod_{\alpha_i = \alpha} P_i$.

par unicité de la décomposition en irréd. dans un anneau factoriel.

Comme Q_α divise $P = \prod_{i=1}^{r} P_i$, il existe $I_\alpha \subset [\![1, r]\!]$ tq $Q_\alpha = \prod_{i \in I_\alpha} P_i$

D'autre part $Q_\alpha \mid V-\alpha$ donc par le lemme de Gauss, on a en fait
$I_\alpha = \{1 \leq i \leq r : P_i \mid V-\alpha\}$ car les P_i sont premiers entre eux 2 à 2.
Or $P_i \mid V-\alpha \iff V-\alpha = 0 \mod P_i \iff \alpha_i = \alpha$.
Donc $I_\alpha = \{1 \leq i \leq r : \alpha_i = \alpha\}$, d'où $Q_\alpha = \prod_{\alpha_i = \alpha} P_i$.

$\{1, \dots, r\} = \coprod_{\alpha \in \mathbb{F}_q} I_\alpha$

Ainsi $P = \prod_{i=1}^{r} P_i = \prod_{\alpha \in \mathbb{F}_q} \underbrace{\prod_{i \in I_\alpha} P_i}_{Q_\alpha} = \prod_{\alpha \in \mathbb{F}_q} \text{pgcd}(P, V-\alpha)$.

l'algorithme termine en un nb. fini d'étapes.

Montrons enfin que r diminue strictement à chaque étape.
Le choix d'un $V \in \mathbb{F}_q[X]$ non constant mod P montre qu'il existe $i \neq j$ tq $\alpha_i \neq \alpha_j$. Ainsi, au moins deux des facteurs apparaissant dans
$P = \prod_{\alpha \in \mathbb{F}_q} \text{pgcd}(P, V-\alpha)$ sont non triviaux et donc ont chacun strictement moins de r facteurs irréductibles.
Par ailleurs chaque nouveau polynôme est un diviseur de P donc est sans carré. □

Cas général.

Lemme: k corps fini de caractéristique p et $P \in k[X]$.
Alors $P' = 0 \iff \exists R \in k[X],\ P = R^p$.

Dém: on écrit $P = \sum_{i=0}^{\ell} a_i X^i$. On a donc $P' = 0 \iff a_i = 0\ \forall i \nmid p$.
En effet si $a_k X^k$ est un monôme avec $a_k \neq 0$, $P' = 0 \Rightarrow k a_k = 0$
Par intégrité, on doit avoir $k \mod p = 0$.
Bref $P' = 0 \iff P = \sum_{j=0}^{s} a_{pj} X^{pj}$. Comme k est un corps fini de caractéristique p, le Frobenius est surjectif i.e $\exists b_j \in k$ tq $a_{pj} = b_j^p$
et avec Frobenius, on a $P = \left(\sum_{j=0}^{s} b_j X^j\right)^p$.
On peut par exemple prendre $b_j = a_j^{p^{(n-1)}}$. □

Rmq : $\mathrm{pgcd}(P, P') = 1 \iff P$ est sans facteur carré.

Dans un corps fini k de carac. p, on a par le lemme :

$\mathrm{pgcd}(P, P') = P \iff P' = 0 \iff \exists R \in k[X]$ tq $P = R^p$.

On obtient R en calculant la racine $p^{\text{ème}}$ des coefficients de P.

Algo : Si P est à coefficients dans un corps fini k de caractéristique p.

i) si P est constant, ok.

ii) on calcule $\mathrm{pgcd}(P, P')$.

- si $\mathrm{pgcd}(P, P') = 1$, on applique Berlekamp à P.
- si $\mathrm{pgcd}(P, P') = P$, on calcule $R \in k[X]$ tq $P = R^p$ et on recommence avec R.
- sinon, $\mathrm{pgcd}(P, P')$ et $\dfrac{P}{\mathrm{pgcd}(P, P')}$ sont deux facteurs non triviaux de P : on recommence avec eux.

Exemple : (à mettre en appli dans le plan)

Montrons que $P = X^p - X - 1 \in \mathbb{F}_p[X]$ est irréductible.

P est sans facteur carré car $P' = -1$ donc $\mathrm{pgcd}(P, P') = 1$.

$S_p : X \bmod P \longmapsto X^p \bmod P$.

$S_p(X^k) = X^{pk} \bmod P = (X+1)^k \bmod P = \sum_{i=0}^{k} \binom{k}{i} X^i \bmod P$

donc $\mathrm{Mat}_{\mathcal{B}}(S_p) = \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ et $\mathrm{Mat}_{\mathcal{B}}(S_p - \mathrm{Id}) = \begin{pmatrix} 0 & & * \\ & \ddots & \\ & & 0 \end{pmatrix}$

donc $\dim(\mathrm{Ker}(S_p - \mathrm{Id})) = 1$.