TP5 : Factorisation complète de polynômes univariés

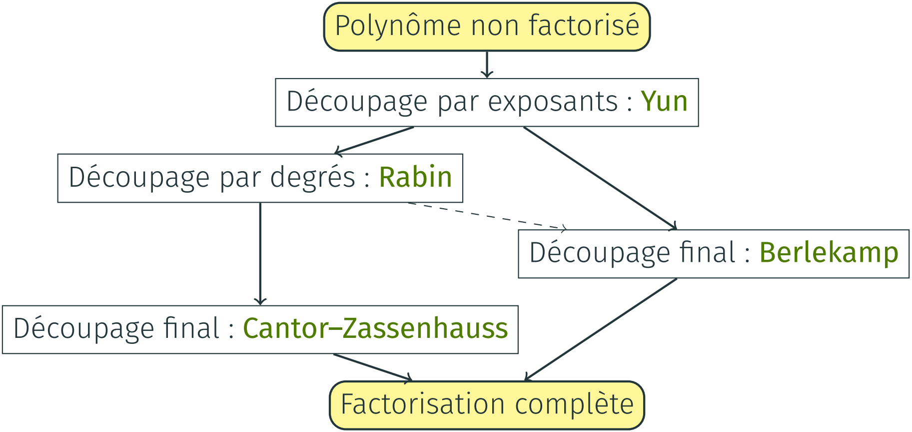
Résumé du TP

Bertrand Meyer

11 décembre 2019

La factorisation sur un corps fini

On souhaite **factoriser** un polynôme $f \in \mathbb{F}_q[x]$.



Algorithme de Berlekamp

Idée

Si $f = \prod_{i=1}^{k} f_i$, on a

$$\mathbb{F}_q[x]/\langle f \rangle \quad = \quad \bigoplus_{k=1}^{k} \mathbb{F}_q[x]/\langle f_i \rangle$$

Donc $f \wedge h$ non trivial si $h \equiv 0 \mod f_i$ pour la moitié des f_i.

Mais

$$\mathbb{F}_q[x]/\langle f \rangle \quad = \quad \bigoplus_{k=1}^{k} \mathbb{F}_{q^{\deg f_i}} \supseteq \bigoplus_{k=1}^{k} \mathbb{F}_q$$

où $\mathcal{B} = \bigoplus_{k=1}^{k} \mathbb{F}_q$ est calculable par algèbre linéaire : $\ker(g \mapsto g^q - g)$.

Si $b \in \mathcal{B}$, $b - \alpha$ s'annule dans $\mathbb{F}_q[x]/\langle f_i \rangle$ pour l'un des $\alpha \in \mathbb{F}_q$.
$\rightarrow$ fournit des candidats pour h.

Algorithme de Berlekamp

1. Ecrire la matrice $\mathbf{Q}$ (Petr-Berlekamp) de l'application

$$\begin{cases} \mathbb{F}_q[x] & \to & \mathbb{F}_q[x] \\ g & \mapsto & g^q - g \end{cases}$$

2. Chercher le noyau $\mathbf{b}_1, \ldots, \mathbf{b}_k$ de $\mathbf{Q} - \mathbf{I}_n$.
3. Pour tout $1 \leq i \leq k$ et tout $\alpha \in \mathbb{F}_q$,
   calculer $h \wedge (\mathbf{b}_i - \alpha)$ où h est un facteur déjà trouvé de f.
   remplacer h par les deux facteurs trouvés.
   s'arrêter quand on a obtenu k facteurs.
4. Renvoyer la liste des facteurs

Exemple

$f = x^4 + x^3 + x^2 + 1 \in \mathbb{F}_4[x]$ à factoriser.

$$\mathbf{Q} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \text{ car } \begin{cases} (1)^4 & = & 1 & \mod f \\ (x)^4 & = & x^3 + x^2 + 1 & \mod f \\ (x^2)^4 & = & x & \mod f \\ (x^3)^4 & = & x^2 + x + 1 & \mod f \end{cases}$$

$$\ker(\mathbf{Q} - \mathbf{I}_4) = \text{Vect}(\underbrace{1}_{\mathbf{b}_1}, \underbrace{x + x^3}_{\mathbf{b}_2}) \quad \to \quad 2 \text{ facteurs.}$$

Avec $\alpha = 1$, $f \wedge (\mathbf{b}_2 - \alpha) = x^3 + x + 1$, d'où

$$f = (x + 1)(x^3 + x + 1).$$

Factorisation dans $\mathbb{Z}[x]$

Une idée insuffisante

Espoir :
Factoriser dans $\mathbb{Z}/m\mathbb{Z}[x]$ révèle la factorisation dans $\mathbb{Z}[x]$ quand m est grand

Contre-exemple
x^4+1 est irréductible dans $\mathbb{Z}[x]$ mais dans $\mathbb{F}_p[x]$

$$x^4+1=\begin{cases} \prod_{\pm}\left(x-\frac{\sqrt{2}}{2}(\pm 1\pm\sqrt{-1})\right) & \text{si } p\equiv 1[8] \\ (x^2-\sqrt{-2}x-1)(x^2+\sqrt{-2}x-1) & p\equiv 3[8] \\ (x^2-\sqrt{-1})(x^2+\sqrt{-1}) & p\equiv 5[8] \\ (x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1) & p\equiv 7[8] \end{cases}$$

Meilleure manière :
Factoriser dans $\mathbb{Z}/m\mathbb{Z}[x]$ puis regrouper pour en faire des facteurs dans $\mathbb{Z}[x]$

Le relèvement de Hensel

Principe :
Un début de factorisation dans $\mathbb{Z}/m\mathbb{Z}$ peut s'étendre dans $\mathbb{Z}/m^2\mathbb{Z}$.

On part d'une factorisation

$$f = gh \in \mathbb{Z}/m\mathbb{Z}[x]$$

On obtient d'une factorisation

$$f = \hat{g}\hat{h} \in \mathbb{Z}/m\mathbb{Z}[x]$$

avec $g = \hat{g}$, $h = \hat{h}$ modulo m.

En réitérant le procédé, on peut arriver dans $\mathbb{Z}/M\mathbb{Z}$ pour M aussi grand que voulu.

Trouver des facteurs de f avec LLL

Principe :
Si $\|f\|$ et $\|g\|$ petits devant m et f, g possèdent un diviseur commun u dans $\mathbb{Z}/m\mathbb{Z}$, alors $f \wedge g$ n'est pas trivial.

Utilisation :
On travaille à l'envers.

On fabrique g à partir u, où u est l'un des facteurs de f dans $\mathbb{Z}/m\mathbb{Z}[x]$.

g un vecteur court du réseau $\mathbb{Z}[x] \cdot u \oplus \mathbb{Z}[x] \cdot m$.