

CM11 : Factorisation dans $\mathbb{Z}/p\mathbb{Z}[x]$

On souhaite décomposer un polynôme $F(x)$ en produit de facteurs irréductibles dans $\mathbb{Z}/p\mathbb{Z}[x]$. Pour la simplicité de l'exposé on supposera $F(x)$ sans facteur multiple, on peut toujours se ramener à ce cas (voir le TP 8), un critère simple est donné par le lemme suivant :

Lemme : soit k un corps et $F(x)$ un polynôme dans $k[x]$, $F(x)$ est sans facteur multiple si et seulement si $\text{pgcd}(F(x), F'(x)) = 1$.

On peut démontrer que

Proposition : L'application $\mathcal{B} : g(x) \rightarrow g^p(x) - g(x) \pmod{F(x)}$ de $\mathbb{Z}/p\mathbb{Z}[x]/(F(x))$ dans lui-même est une application linéaire.

et si la décomposition de $F(x)$ en produit de facteurs irréductibles est $F_1(x) \times \dots \times F_k(x)$ où les $F_i(x)$ sont irréductibles et premiers entre eux puisque $F(x)$ est sans facteur multiple

Théorème : les éléments du noyau de \mathcal{B} sont les solutions des problèmes chinois :

$g(x) = a_1 \pmod{F_1(x)}, \dots, g(x) = a_k \pmod{F_k(x)}$ où les $a_i \in \mathbb{Z}/p\mathbb{Z}$.

En particulier la dimension du noyau est k le nombre de facteurs irréductibles.

Un exemple dans $\mathbb{Z}/2\mathbb{Z}[x]$

Soit $F(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ dans $\mathbb{Z}/2\mathbb{Z}[x]$

1. $F(x)$ est-il sans facteur multiple ? On calcule le $\text{pgcd}(F(x), F'(x))$:

$F'(x) = x^4 + x^2 + 1$ et $F(x) = F'(x)(x^2 + x) + 1$ donc $\text{pgcd}(F(x), F'(x)) = 1$.

$F(x)$ est sans facteur multiple.

2. On calcule la matrice de l'application \mathcal{B} dans la base $1, x, x^2, x^3, x^4, x^5$ de $\mathbb{Z}/2\mathbb{Z}[x]/(F(x))$:

l'image de 1 est 0, celle de x est $x^2 - x = x^2 + x$, celle de x^2 est $x^4 - x^2 = x^4 + x^2$,

celle de x^3 est $x^6 - x^3 \pmod{F(x)} = x^5 + x^4 + x^2 + x + 1$,

celle de x^4 est $x^8 - x^4 \pmod{F(x)} = x^4 + x$,

celle de x^5 est $x^{10} - x^5 \pmod{F(x)} = x^5 + x^3$.

Il est astucieux pour faire les deux derniers calculs de réutiliser le calcul précédent.

On a donc la matrice

$$\mathcal{B} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

3. Il faut calculer une base du noyau de \mathcal{B} . Les équations sont

$$\begin{cases} a_3 & = & 0 \\ a_1 + a_3 + a_4 & = & 0 \\ a_1 + a_2 + a_3 & = & 0 \\ a_5 & = & 0 \\ a_2 + a_3 + a_4 & = & 0 \\ a_3 + a_5 & = & 0 \end{cases} \quad \text{qui se réduisent au système libre} \quad \begin{cases} a_3 & = & 0 \\ a_5 & = & 0 \\ a_1 + a_2 & = & 0 \\ a_1 + a_4 & = & 0 \end{cases}$$

Attention la réduction doit être faite dans $\mathbb{Z}/2\mathbb{Z}$.

La dimension du noyau est donc 2 (défini par 4 équations indépendantes dans un espace de dimension 6), on sait donc que $F(x)$ est le produit de deux facteurs irréductibles.

Une base possible du noyau est formée du vecteur $(1\ 0\ 0\ 0\ 0\ 0)$ qui correspond aux constantes et qu'on retrouvera dans le noyau de \mathcal{B} quelque soit le polynôme $F(x)$ et du vecteur $(0\ 1\ 1\ 0\ 1\ 0)$ qui correspond au polynôme $g(x) = x^4 + x^2 + x$.

4. On sait que $F(x)$ divise $g^2(x) - g(x) = g(x)(g(x) - 1)$. En calculant les $\text{pgcd}(F(x), g(x))$ et $\text{pgcd}(F(x), g(x) - 1)$ on obtiendra les facteurs irréductibles de $F(x)$.

On calcule le $\text{pgcd}(F(x), g(x))$:

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^4 + x^2 + x)(x^2 + x) + x^3 + x + 1$$

$$x^4 + x^2 + x = (x^3 + x + 1)x + 0$$

Donc $\text{pgcd}(F(x), g(x)) = x^3 + x + 1$ et on a le premier facteur de $F(x)$.

Pour obtenir le second facteur on peut calculer le $\text{pgcd}(F(x), g(x) - 1)$ mais il est plus simple de diviser $F(x)$ par le premier facteur trouvé :

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x + 1)(x^3 + x^2 + 1) \text{ et on a la décomposition de } F(x) \text{ en facteurs irréductibles.}$$