UNIVERSITÉ MONTPELLIER 2
SCIENCES ET TECHNIQUES

FLMA607 Calcul Formel – 2010–2011

Feuille de TD n°3 : Factorisation de polynômes.

Exercice 1 (Critère d'Eisenstein)

1) Soit $f(x) = a_n x^n + \cdots + a_0$ un polynôme de $\mathbb{Z}[x]$ et soit p un nombre premier. On suppose que
   a) les coefficients $a_0, \ldots, a_{n-1}$ sont divisibles par p ;
   b) a_n n'est pas divisible par p ;
   c) a_0 n'est pas divisible par p^2.

Montrer que f est irréductible dans $\mathbb{Q}[x]$.
2) Montrer que pour tout $n \in \mathbb{N}^*$ le polynôme $x^n - p$ est irréductible sur $\mathbb{Q}$.
3) Montrer que $55x^4 + 420x^3 + 28$ est irréductible sur $\mathbb{Q}$.

Exercice 2

Quelle factorisation donnera l'algorithme de décomposition sans facteur carré pour le polynôme $x^4(x+1)^3$?

Exercice 3

Parmi les polynômes suivants, déterminer ceux qui sont sans facteur carré. Justifier les réponses.

- $f_1(X) = X^3 + 2 \in \mathbb{F}_3[X]$;
- $f_2(X) = 2X^3 + 2X^2 + X + 1 \in \mathbb{F}_3[X]$;
- $f_3(X) = 2X^3 + 2X^2 + X + 2 \in \mathbb{F}_3[X]$.

Exercice 4

Calculer la décomposition sans facteur carré des polynômes suivants dans $\mathbb{Q}[x]$ et dans $\mathbb{F}_3[x]$.

(i) $x^6 - x^5 - 4x^4 + 2x^3 + 5x^2 - x - 2$
(ii) $x^6 - 3x^5 + 6x^3 - 3x + 2$
(iii) $x^5 - 2x^4 - 2x^3 + 4x^2 + x - 2$

Exercice 5

Soient p un nombre premier, q une puissance de p et $f = f_1 \ldots f_r \in \mathbb{F}_q[x]$ un polynôme sans facteur carré où les f_i sont unitaires et irréductibles. Soit $\mathcal{B} \subset \mathbb{F}_q[x]/(f)$ la sous-algèbre de Berlekamp de f.
1) Montrer que pour tout i, il existe un unique polynôme $l_i \in \mathbb{F}_q[x]$ de degré $< \deg f$ et tel que $l_i \equiv 0 \mod f_j$ si $j \neq i$ et $l_i \equiv 1 \mod f_i$.
2) Montrer que les l_i forment une base de $\mathcal{B}$.

Exercice 6

Soit $f = x^3 + 4x^2 + 4x + 3 \in \mathbb{F}_5[x]$.
1) Donner la matrice, dans la base $1, x, x^2$, de l'application linéaire $\sigma : \mathbb{F}_5[x]/(f) \to \mathbb{F}_5[x]/(f)$ définie par $\sigma(P) = P^5 - P$.
2) Au fait, pourquoi σ est-elle linéaire ?
3) Calculer le rang de σ.
4) En déduire le nombre de facteurs irréductibles de f.
5) Vérifier votre résultat en factorisant f.

Exercice 7 (extrait de l'examen 2010)

On cherche à factoriser le polynôme $f = x^4 + x^3 + 5x^2 + 5x + 12$ dans $\mathbb{Z}[x]$. On admet que les coefficients des facteurs irréductibles de f sont tous majorés par 5 en valeur absolue. On notera $\overline{f} \in \mathbb{F}_{11}[x]$ la réduction de f modulo 11. On pourra utiliser les relations suivantes (les égalités polynomiales ont lieu dans $\mathbb{F}_{11}[x]$) :

$$\begin{aligned}
\Delta(f) &= \operatorname{Res}(f, f') = 2^5.3.5.17^2 \\
x^{11} &\equiv 10x^3 + 9x^2 + 9x \mod \overline{f} \\
x^{22} &\equiv 10x^3 + 10x^2 + 8x \mod \overline{f} \\
x^{33} &\equiv 4x^3 + 6x^2 + 9x \mod \overline{f} \\
(x^2 - x + 9)^5 &\equiv 9x^3 + 4x^2 + x + 9 \mod \overline{f} \\
\overline{f} &= (5x + 4)(9x^3 + 4x^2 + x + 9) + 6x^2 + 9
\end{aligned}$$

1) Écrire la matrice qui permet de calculer $\Delta(f)$.
2) On pose $p = 11$ et on décide de commencer par factoriser l'image $\overline{f}$ de f dans $\mathbb{F}_p[x]$. Expliquer ce choix de p. Parmi les entiers de 1 à 20, lesquels aurait-on pu choisir ?
3) Calculer la matrice de l'application linéaire

$$L\colon \begin{cases} \mathbb{F}_p[x]/(f) \longrightarrow \mathbb{F}_p[x]/(f) \\ G \longmapsto G^p - G \end{cases}$$

dans la base $1, x, x^2, x^3$.
4) Donner une base de la sous-algèbre de Berlekamp $\mathcal{B} \subset \mathbb{F}_p[x]/(f)$. Combien $\overline{f}$ a-t-il de facteurs irréductibles ?
5) En utilisant l'algorithme de Berlekamp, factoriser complètement $\overline{f}$ dans $\mathbb{F}_p[x]$. (On pensera à utiliser les relations données ci-dessus pour alléger les calculs.)
6) En déduire la factorisation de f dans $\mathbb{Z}[x]$.

Exercice 8

Soit $f = x^4 + x^3 + x - 1 \in \mathbb{F}_3[x]$.
1) Montrer que f est séparable.
2) Combien l'algèbre $A = \mathbb{F}_3[x]/(f)$ a-t-elle d'éléments ?
3) Calculer la sous-algèbre de Berlekamp $\mathcal{B}$ de A (donner une base). Combien comporte-t-elle d'éléments ?
4) Un élément de A correspond à un polynôme $a_0 + a_1x + a_2x^2 + a_3x^3$. On représentera A par un tableau à deux entrées avec $a_0 + a_1x$ en abscisse et $a_2x^2 + a_3x^3$ en ordonnée. Colorier dans ce tableau les cases correspondant aux éléments de $\mathcal{B}$.
5) Combien f a-t-il de facteurs irréductibles ?
6) Factoriser f par la méthode de Berlekamp (non améliorée).
7) En déduire un isomorphisme $A \simeq A_1 \times A_2$ par le théorème chinois.
8) Faire la liste des éléments de A_1 et A_2 puis représenter de nouveau A par un tableau à deux entrées, en mettant cette fois-ci les éléments de A_1 en abscisse et ceux de A_2 en ordonnée. Dessiner $\mathcal{B}$ dans ce nouveau tableau.
9) Exécuter à la main l'algorithme de Berlekamp amélioré (*i.e.* la version probabiliste) sur le polynôme f. Dans les tableaux des questions 3 et 7, marquer d'une croix les cases qui correspondent aux choix « chanceux » (*i.e.* ceux qui conduisent à une factorisation non triviale de f).

Exercice 9

Soit $f = x^5 + 14x^4 + 5x^3 + 7x^2 + 6x + 2 \in \mathbb{Z}[x]$. Pour quels nombres premiers p la réduction modulo p de f est-elle sans facteur carré dans $\mathbb{F}_p[x]$? (On donne $\Delta(f) = 2^3.5.11^2.103.1321$.)

Exercice 10

1) Calculer par la méthode de Cantor-Zassenhaus la factorisation du polynôme $f = x^4+6x^3+5x^2-12x+3 \in \mathbb{Z}[x]$ dans $\mathbb{F}_{11}[x]$. On admettra que : $\operatorname{pgcd}(9x + 8, f) \equiv 1 \bmod 11$, que $x^{121} \equiv x \bmod f$ et que $(x^2 + 1)^{60} \equiv x^2 + 3x + 9 \bmod f$.
2) Retrouver cette factorisation par la méthode de Berlekamp. On admettra que, dans $\mathbb{F}_{11}[x]$,

$$\begin{aligned} x^{11} &\equiv 10x + 8 \mod f \\ x^{22} &\equiv x^2 + 6x + 9 \mod f \\ x^{33} &\equiv 10x^3 + 2x^2 + 6x + 6 \mod f \\ (x^2 + 3x + 1)^5 &\equiv x^2 + 3x + 9 \mod f \end{aligned}$$

3) Factoriser f dans $\mathbb{Z}[X]$ sachant que la factorisation obtenue est de la forme $f = g_1g_2$ avec g_1 et g_2 deux polynômes irréductibles dans $\mathbb{Z}[x]$ dont les coefficients sont bornés en valeur absolue par 5.

Exercice 11

Soit $f = X^4 + X^3 - 14X^2 + 13X - 3 \in \mathbb{Z}[X]$. Le polynôme f se factorise dans $\mathbb{F}_3[X]$ sous la forme $f \equiv X(X^2 + 1)(X + 1) \bmod 3$. Calculer une factorisation de f dans $\mathbb{Z}[X]$ sachant que les coefficients des facteurs irréductibles de f sont bornés en valeur absolue par 4.