Université de Lorraine, site de Metz
Département de Mathématiques

Année universitaire 2014-2015.

L3 Calcul formel

Feuille de TD n° 3

Exercice 1

En utilisant l'algorithme de Berlekamp, factoriser
1) dans $\mathbb{F}_5[X]$ le polynôme $F = X^4 - X^3 - X^2 + 2X - 2$.
2) dans $\mathbb{F}_3[X]$ le polynôme $F = X^{12} - X^9 - X^3 - 1$.
3) dans $\mathbb{F}_7[X]$ le polynôme $F = X^5 + X^4 + 2X^3 + 2X^2 + 2X + 2$.

Exercice 2

Soit $A = X^4 - 2X^3 - 7X^2 - 16X + 15$.

1. Vérifier que $\phi_7(A) = (X^2 + 3X - 2)(X^2 + 2X + 3)$ est la décomposition de A en produit de polynômes irréductibles de $\mathbb{F}_7[X]$.
2. Donner une majoration des coefficients des diviseurs éventuels de A dans $\mathbb{Z}[X]$.
3. Appliquer le lemme de Hensel pour trouver la décomposition de A en produit de polynômes irréductibles de $\mathbb{Z}[X]$.

Exercice 3 (Janvier 2014)

Factoriser dans $\mathbb{Z}[X]$ le polynôme $F = X^4 + 9X^3 - 3X^2 - 102X + 130$.

Exercice 4 (Janvier 2015)

Factoriser dans $\mathbb{Z}[X]$ le polynôme $F = X^4 - 16X^3 + 9X^2 + 192X - 252$.

Exercice 5

Soit le polynôme $F = X^8 + X^4 + 1$.

1. (a) Quel est le polynôme unitaire irréductible de $\mathbb{Z}[X]$ annulé par $j = e^{i\frac{2\pi}{3}}$? On le note F_1. Quel est le polynôme unitaire irréductible de $\mathbb{Z}[X]$ annulé par $-j$? On le note F_2.
   (b) Montrer que j et $-j$ sont racines de F.
   (c) En déduire que le produit $F_1.F_2$ divise F.
   (d) Trouver un polynôme G de $\mathbb{Z}[X]$, unitaire tel que $F = G.F_1.F_2$.
2. En utilisant l'algorithme de Berlekamp, factoriser le polynôme F dans $\mathbb{F}_5[X]$.
3. Donner une majoration des coefficients des diviseurs éventuels de G dans $\mathbb{Z}[X]$.
4. En utilisant le lemme de Hensel, déterminer la décomposition de G en produit de polynômes irréductibles de $\mathbb{Z}[X]$.
5. En déduire la factorisation de F dans $\mathbb{Z}[X]$.

Exercice 6

Soit $F = X^4 - 6X^3 - 221X^2 + 540X - 300$ dans $\mathbb{Z}[X]$.

1. Factoriser $\phi_p(F)$ pour p=3, 5, 7.
2. Choisir un p convenable et appliquer le lemme de Hensel pour factoriser F dans $\mathbb{Z}[X]$.