Algèbre et Calcul Formel

Examen Final

24 avril 2013, durée 3h

Documents interdits, calculatrices autorisées

Exercice 1 : Nous avons vu en cours des algorithmes permettant de factoriser un polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, où p est un nombre premier. Soit $f \in \mathbb{Z}[x]$, on sait donc factoriser f modulo p. Dans cet exercice nous allons voir comment passer d'une factorisation modulo p à une factorisation modulo p^2. On suppose donc connaitre $g, h \in \mathbb{Z}[x]$ tels que

$$f(x) = g(x)h(x) \bmod p$$

avec $g(x)$ et $h(x)$ premiers entre eux modulo p.

Notation : dans tout ce qui suit, si $P(x) = \sum_i a_i x^i \in \mathbb{Z}[x]$, et $n \in \mathbb{N}$, on note $P(x) \bmod n$ la réduction de P modulo $n\mathbb{Z}[x]$, c'est-à-dire le polynôme $\sum_i r_i x^i \in \mathbb{Z}[x]$ où $r_i \in \{0, 1, \ldots, (n-1)\}$ est le reste de a_i dans la division par n.

1. Justifiez l'existence de deux polynômes $u(x)$ et $v(x)$ appartenant à $\mathbb{Z}[x]$ tels que

$$u(x)g(x) + v(x)h(x) = 1 \bmod p,$$

   et citez un algorithme permettant de les calculer.

2. On pose $e(x) = f(x) - g(x)h(x)$ et

$$\begin{cases} g'(x) = g(x) + v(x)e(x) \\ h'(x) = h(x) + u(x)e(x) \end{cases}$$

   Montrez que $f(x) = g'(x)h'(x) \bmod p^2$.

3. Application numérique : soit $f(x) = x^4 - 1$.
   (a) Vérifiez que $f(x) = (x-2)(x^3 + 2x^2 - x - 2) \bmod 5$. On pose $g = x^3 + 2x^2 - x - 2$ et $h = x - 2$.
   (b) Calculez $u(x)$ et $v(x)$ comme en 1.
   (c) Calculez $e(x)$, puis $g'(x)$ et $h'(x)$ comme en 2.

   Dans cet exemple, on constate que le degré de $g'(x)h'(x)$ est supérieur au degré de f. On va donc modifier la méthode précédente pour contourner ce problème.

4. Justifiez l'existence de deux polynômes $q(x)$, $r(x)$ tels que

$$u(x)e(x) = q(x)h(x) + r(x) \bmod p^2,\ \deg(r) < \deg(h),\ q(x) = r(x) = 0 \bmod p.$$

5. On pose
$$\begin{cases} g^*(x) = g(x) + v(x)e(x) + q(x)g(x) \bmod p^2 \\ h^*(x) = h(x) + u(x)e(x) - q(x)h(x) \bmod p^2 \end{cases}$$
Montrez que $f(x) = g^*(x)h^*(x) \bmod p^2$.
6. Montrez que $\deg(h^*) = \deg(h)$ et que ces deux polynômes ont le même coefficient dominant, puis que $\deg(g^*) = \deg(g)$.
7. Application numérique : appliquez ce qui précède pour donner une factorisation de $x^4 - 1$ modulo 25 en un produit d'un polynôme de degré 1 et d'un polynôme de degré 3.

Exercice 2 : Soit K un corps ; on utilisera les notations : $X = (x_1, \ldots, x_n)$, $K[x_1, \ldots, x_n] = K[X]$, et si $f \in K[x_1, \ldots, x_n]$, $f = f(x_1, \ldots, x_n) = f(X) \in K[X]$. Soit $I = \langle f_1, \ldots, f_s \rangle$ un idéal de $K[X]$ et soit $\sqrt{I}$ l'ensemble :

$$\sqrt{I} := \{f \in K[X] \ : \text{ il existe } m \geq 1 \text{ tel que } f^m \in I\}.$$

Le but de cet exercice, est de donner un algorithme permettant de tester si un polynôme $f(X)$ appartient à $\sqrt{I}$, à partir des données : $\{f_1, \ldots, f_s\}$, et f.

1. Rappeler comment la notion de base de Groebner permet de tester si $f \in I$ (on ne demande pas ici de démonstrations).
2. Montrez que $\sqrt{I}$ est un idéal de $K[X]$ contenant I.
3. Soit
$$J := \langle f_1(x), \ldots, f_s(X), 1 - yf(X) \rangle \subset K[X, y] = K[x_1, \ldots, x_n, y].$$
Dans cette question, on montre l'équivalence :
$$f \in \sqrt{I} \iff 1 \in J.$$
   (a) Montrez que, si $f \in \sqrt{I}$, alors $1 \in J$
   (indication : on pourra partir de l'identité $1 = y^m f^m + (1 - y^m f^m)$).
   (b) Montrez la réciproque (on pourra partir d'une identité de la forme
   $$1 = q_1(X, y)f_1(X) + \cdots + q_s(X, y)f_s(X) + p(X, y)(1 - yf(X))$$
   puis l'évaluer en $y = 1/f(X)$).
4. Proposer à partir de ce qui précède un algorithme permettant de tester si $f \in \sqrt{I}$.