

Réduction modulo p des polynômes, et deux exemples non triviaux. Perrin page 77+Ortiz page

Pierre Lissy

April 9, 2010

On considère P un polynôme à coefficients entiers, on le suppose réductible dans $\mathbb{Q}[X]$. Ecrivons $P = c(P)P'$ avec P' primitif. Alors on peut le décomposer sous la forme $P'(X) = Q(X)R(X)$ avec Q et R pour le moment à coefficients rationnels. Mais si l'on écrit les coefficients de Q par exemple sous la forme (a_i/b_i) avec $\text{pgcd}(a_i, b_i) = 1$, alors en factorisant par $b = \text{ppcm}(b_a, \dots, b_n)$ $Q(X) = 1/bQ'(X)$ et $a = \text{pgcd}(a_1, \dots, a_n)$ puis en simplifiant éventuellement la fraction on obtient $Q(X) = a'/b'Q''(X)$ avec $\text{pgcd}(a', b')$ premiers entre eux et Q'' à coefficients entiers. De même avec R , on obtient $R = a''/b''R''$. On remarque que Q'' et R'' sont primitifs. Mais en écrivant $b'b''P(X) = a'a''Q''(X)R''(X)$ et en passant au contenu on voit que $a'a''/b'b'' = c(P')/C(Q'')C(R'') = 1$. Donc $P(X) = S(X)T(X)$ avec S et T maintenant à coefficients entiers (on multiplie P' par le contenu qui est entier). On réduit modulo p : $\bar{P} = \bar{S}\bar{T}$. Mais $\bar{P}$ est irréductible lui donc $\bar{S}$ ou $\bar{T}$ est de degré 0 et S ou T aussi, d'où l'irréductibilité.

Exemple 1. $X^p - X - 1$ est irréductible dans $\mathbb{Q}[X]$ et donc dans $\mathbb{Z}[X]$ puisqu'il est primitif; En effet il est irréductible dans $\mathbb{F}_p$. Soit α une racine de ce polynôme dans un corps de rupture du polynôme; les autres racines sont alors $\alpha+1, \dots, \alpha+(p-1)$. En effet, d'abord par la caractéristique ces éléments sont deux à deux distinct, de plus par Frobenius $(\alpha+i)^p = \alpha^p + i^p = \alpha+1+i$, ce qui montre bien que c'est une racine. Si on avait la réductibilité, $P = QR$. $Q = \prod_1^d (X - \alpha - i_k)$. Le coefficient devant X^{d-1} est $-(d\alpha + i_1 + \dots + i_d)$ qui doit être dans $\mathbb{F}_p$, ceci implique $d\alpha$ aussi et comme d est non nul on a $\alpha \in \mathbb{F}_p$, pas possible: $\alpha^p = \alpha$ contredit.

Un autre type d'exemple non trivial.

Exemple 2. Ortiz page 148. $P = X^4 + 4X^3 + 3X^2 + 7X - 4$. Modulo 2, le polynôme est réductible. Modulo 3 aussi: $P = (X^2 + 1)(X^2 + X - 1)$ et c'est la décomposition en irréductibles. On arriverait de même pas à réduire modulo 5, 7. On décide donc de changer de méthode et on remarque que grâce à la réduction modulo 3, on voit que le polynôme de départ n'a pas de racines dans $\mathbb{Z}$. La réduction modulo 2 donne $P = X(X^3 + X + 1)$ produit de deux polynômes irréductibles. P ne peut donc se décomposer en un produit de polynôme de degré 2. Il est donc irréductible (si il était réductible, soit il avait une racine dans $\mathbb{Z}$ soit il serait produit de degré 2)