Université Claude Bernard, Ens Lyon 2001-2002
Magistère Math-Info, Calcul formel, TD du 23 novembre 2002

Exercice 1

On se propose d'étudier la factorisation du polynôme $P(x) = x^5 - a$ sur le corps $\mathbb{F}_7$.

1. Montrer que si $a \neq 0$ le polynôme P est sans facteurs carrés.
2. Calculer $x^{7k} \pmod{P(x)}$ pour $0 \leq k \leq 4$, et en déduire la matrice de Berlekamp M de P.
3. Déterminer suivant les valeurs de a le rang de la matrice $M - I$.
4. Dans le cas où $a = 2$, donner la factorisation de $P(x)$ dans $\mathbb{F}_7[x]$.

Exercice 2

Soit f un polynôme de $\mathbb{F}_p[x]$.

1. Ecrire la procédure
   `> berlekamp(f,x,p)`
   qui reçoit le polynôme f et rend une base du noyau de l'endomorphisme $v \to v^p - v$ de l'espace vectoriel quotient $\mathbb{F}_p[x]/(f)$ des classes de congruence modulo f dans $\mathbb{F}_p[x]$.
2. Ecrire la procédure
   `> berlfact := proc(f,x,p)`
   qui reçoit un polynôme de $\mathbb{F}_p[x]$, et le factorise au moyen de la méthode originale de Berlekamp, dans le cas où p n'est pas trop grand.
3. En déduire la factorisation modulo 7 de $x^{60} - 1$. Vérifiez le résultat à l'aide de la commande Maple `Factor(f) mod p`.

Exercice 3

1. Soient α et β deux nombres algébriques, n un entier naturel plus grand que 1, et $P, Q \in \mathbb{Q}[x]$ deux polynômes tels que $P(\alpha) = Q(\beta) = 0$. Ecrire les procédures
   (a) `polyplus := proc(P,Q,x)` qui rend un polynôme de $\mathbb{Z}[x]$ ayant pour racine $\alpha + \beta$.

(b) `polyprod := proc(P,Q,x)` qui rend un polynôme de $\mathbb{Z}[x]$ ayant pour racine $\alpha\beta$.

(c) `polyrad := proc(P,n,x)` qui rend un polynôme de $\mathbb{Z}[x]$ ayant pour racine $\sqrt[n]{\alpha}$.

2. En déduire une procédure

   > `polyannulateur := proc(e,x)`

   qui reçoit une expression e formée à l'aide d'entiers, d'identificateurs, d'additions, de multiplications et d'extraction de radicaux, autrement dit une expression engendrée par la grammaire

```
<exp> := entier | identificateur | <exp> + <exp>
         | <exp * exp> | <exp> ^ <1/entier>
```

   et qui rend un polynôme de $\mathbb{Z}[x]$ dont e est racine.

3. Ecrire la procédure

   > `nettoie := proc(a,A,x)`

   qui reçoit un polynôma $A \in \mathbb{Z}[x]$ et a une racine de A, et renvoie le facteur irréductible de A qui admet a pour racine. A l'aide de cette procédure modifier la procédure `polyannulateur` pour la transformer en une procédure

   > `polymin := proc(e,x)`

   qui reçoit une expression en radicaux, et rend le polynme minimal de cette expression.

4. Application : soit les nombres

$$\begin{aligned} \alpha &= \sqrt{5} + \sqrt{22 + 2\sqrt{5}} \\ \beta &= \sqrt{11 + 2\sqrt{29}} + \sqrt{16 - 2\sqrt{29} + 2\sqrt{55 - 10\sqrt{29}}}. \end{aligned}$$

   Explicter les polynômes minimaux de A et B, et en déduire que $\alpha = \beta$.