Université Claude Bernard LYON 1
Master MA Mathématiques générales
Algèbre et calcul formel

# Fiche de TP 3

**Exercice 1.**

1. Ecrire une fonction PYTHON ou une procédure MAPLE *racines* qui étant donnés un entier premier $p$ et un entier $m \geq 1$, calcule la *liste* $N$ des diviseurs $n$ de $p^m - 1$ tels que $m$ soit l'ordre de $\overline{p}$ dans le groupe $(\mathbb{Z}/\mathbb{Z}n)^\times$.
2. Calculer $N$ pour $p = 5$ et $m = 6$.
3. Pour tout $n \in N$ déterminer le nombre de facteurs irréductibles de $\overline{\Phi_n} \in \mathbb{F}_p[X]$.
4. Combien existe-t-il de corps finis $K$ *distincts* tels que $\mathrm{Card}(K) = 15625$ ?

**Exercice 2.**

1. Construire un corps fini $K = \mathbb{F}_p[x]$ tel que $\mathrm{Card}(K) = 15625$ et que $x$ soit un élément d'ordre 252 de $K^\star$.
2. On considère $z_1 = x^5 + 2x^2 + x + 3 \in K^\star$ ; vérifier qu'il existe $k$ tel que $z_1 = x^k$.
   L'algorithme de Shanks (*pas de géant-pas de bébé*) permet d'améliorer l'algorithme naïf (qui consiste à essayer toutes les puissances $x^k$ de $x$ pour $0 \leq k \leq n-1$.
   On fixe $d < [\sqrt{n}]$ ; pour tout $k$ on a $k = dq + r$ avec $0 \leq r \leq d-1$. Alors la relation $z = x^k$ se récrit $x^r = z\, x^{-dq}$. L'algorithme consiste, dans un premier temps, à construire le tableau $U$ de toutes les puissances $x^r$ pour $0 \leq r \leq d-1$ (*les pas de bébé*) puis le tableau $V$ de toutes les puissances $x^{-dq}$ pour $1 \leq q \leq [n/d]$ (*les pas de géant*).
   Ensuite on cherche si $z\,v$ pour $v = x^{-dq}$ parcourant $V$ figure dans $U$ *ie.* est de la forme $v = x^r$. Si c'est la cas on a $z = x^k$ avec $k = dq + r$ sinon $z$ n'appartient pas au sous-groupe cyclique engendré par $x$.
3. On prend $z_2 = 3x^4 + 3x^3 + x^2 + 2x + 4 \in K^\star$. Vérifier que $z_2 \notin \langle x \rangle$.