## Polynômes irréductibles. Test de Lucas. Polynômes primitifs

1. Ecrire la procédure

   > `irreductibles := proc(x,p,n)`

   qui rend la liste des polynomes irréductibles de degré $n$ de $\mathbb{F}_p[x]$, où $\mathbb{F}_p$ est le corps $\mathbb{Z}/p\mathbb{Z}$.

2. Ecrire, en utilisant le théorème de Lucas, et la fonction `PrimeDivs(n)`, utilisée dans la fiche 2, qui rend les diviseurs premiers de l'entier $n$, la fonction

   > `generateur:= proc(f,g,x,p)`

   qui rend vrai si et seulement si, $f$ est un polynôme irréductible dans $\mathbb{F}_p[x]$, et si le polynôme $g \in \mathbb{F}_p[x]$ est un générateur du groupe multiplicatif $(\mathbb{F}_p[x]/f\mathbb{F}_p[x])^\times$.

3. On dit qu'un polynôme $f \in \mathbb{Z}[x]$ est un polynôme *primitif modulo* $p$, si

   (a) $f$ est irréductible dans $\mathbb{F}_p[x]$.

   (b) Dans le corps $\mathbb{F}_p[x]/(f)$, la classe de $x$ est un générateur du groupe multiplicatif des éléments non nuls.

   Écrire une procédure

   > `primitif(f,x,p)`

   qui rend vrai si et seulement si $f$ est primitif modulo $p$, et donnez la liste des polynômes primitifs de degré 4 modulo 3.

Vérifiez en utilisant la fonction MAPLE prédéfinie : `Primitive`.

## La fonction de Zech

1. Soit $F_q$ un corps fini à $q$ éléments et $g$ un générateur du groupe multiplicatif $F_q^\star$. On appelle *fonction de Zech* de base $g$, de l'entier naturel $a$ l'entier $z(a)$, défini, pour $a \neq (q-1)/2$ (auquel cas $1 + g^a = 0$), par

   $$1 + g^a = g^{z(a)}.$$

   Ecrire la procédure

   > `tabule_zech := proc(f,g,x,p)`

   qui construit la table des valeurs de la fonction de Zech en base $g$ dans le corps $\mathbb{F}_p[x]/(f)$.