# ALGORITHMIQUE DE BASE - TP N. 4

## 1. Réduction modulo N

**Exercice 1 : Réduction de Barret**

**Rappel :** On cherche à calculer $M \mod N$ sans diviser par $N$, avec $M = \overline{M_{2n-1} \dots M_0}^{(b)}$ $N = \overline{N_{n-1} \dots N_0}^{(b)}$ et $N_{n-1} \neq 0$.

(1) On calcule (une fois pour toutes si on a plusieurs $M$ à reduire) $R = \lfloor b^{2n}/N \rfloor$;
(2) On calcule $q = \lfloor \lfloor (M/b^{n-1}) \rfloor R / b^{n+1} \rfloor$;
(3) On calcule $r = M(\mod b^{n+1}) - qN(\mod b^{n+1})$ (si $r < 0$ on remplace $r$ par $r + b^{n+1}$).
(4) Tant que $r \geq N$ on remplace $r$ par $r - N$.
(5) On retourne $r$.

**Remarque :** Noter que cet algorithme est utile quand on travaille en multi-précision en base $b$ (car les division par $b^i$ deviennent juste des décalages).

## 2. Méthode de Newton

**Exercice 2 : Algorithme de Newton sur $\mathbb{R}$ et $\mathbb{C}$**

**Rappel :** Soit $x_0$ le point initial.
L'itération de Newton est donnée par
$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

Écrire une procedure Maple qui, étant données une fonction `f` et un point initial `a`, applique la recursion de Newton pour chercher une solution de l'equation $f(x) = 0$.
Le programme devra s'arrêter à une des deux conditions suivantes :

(1) Soit la distance $|x_{n+1} - x_n|$ est suffisamment petite (par rapport à la précision fixée), alors on a trouvé une solution;
(2) soit après un nombre fixé d'itérations (exemple : 30), dans ce deuxième cas on donne un message d'erreur.

Tester le programme sur les fonctions suivantes :

- $x^3 + x - 2$
- $(x-1)\ln(x)$
- $x + e^x + \frac{10}{1+x^2} - 5$
- $x^3 + i$.
- $sin(x)$

(TOURNEZ SVP)

*Date*: 18 novembre 2010.

**Exercice 3 : Inversion de polynômes modulo $x^l$**

Soit $P(x) \in \mathbb{Z}[x]$, $P(0) = 1$, $l > 0$.
On cherche un polynôme $Q(x) \in \mathbb{Z}[x]$ tel que

$$PQ \equiv 1 \mod x^l \tag{1}$$

Soit $Q_0 \in \mathbb{Z}[x]$ tel que $PQ_0 \equiv 1 \mod X$. Considérer la relation de récurrence :

$$Q_{i+1} \equiv 2Q_i - PQ_i^2 \mod x^{2^{i+1}}.$$

Alors pour tout $i$ on a

$$PQ_i \equiv 1 \mod x^{2^i}.$$

Écrire une procedure Maple pour résoudre (1).
En particulier calculer l'inverse :

- De $P = 1 + 2x + x^2 + 8x^3 + 4x^4 + 7x^5$ modulo $x^{16}$.

Modifier l'algorithme pour qu'il prenne en argument supplémentaire un premier $p$ et calcule l'inverse modulo $x^l$ dans $\mathbb{F}_p$.

- De $P = 3x^2 + 2x + 1 \in \mathbb{F}_7[x]$ modulo $x^4$.