Soit un modulo $m \in \mathbb{N}^*$.

Soit un polynôme Q à coefficients réels, de degré $n \geq m$ et de forme standard :

$$Q_n(X) = \sum_{k=0}^{n} c_k X^k$$

Alors il existe un unique polynôme P_m de degré au plus $m-1$ tel que :

$$\forall x \in \mathbb{Z}, \tilde{P}_m(Q_n)(x[m]) = \tilde{Q}_n(x[m])$$

Démonstration

Posons :

$$\forall i \in [\![0, m-1]\!], (x_i, y_i) = \left(i, \tilde{Q}_n(i)\right)$$

Par interpolation lagrangienne, l'unique polynôme $P_m(Q_n)$ satisfaisant :

$$\forall i \in [\![0, m-1]\!], \tilde{P}_m(x_i) = y_i \text{ et} \deg(P_m) \leq m-1$$

A pour forme standard :

$$P_m(Q_n)(X) = \sum_{k=0}^{m-1} c_L(m,k) \cdot X^k$$

Avec :

$$\begin{cases} c_L(m,k) = \sum_{j=0}^{m-1} \tilde{Q}_n(j) \cdot c_\ell(m,k,j) \\ c_\ell(m,k,j) = \frac{1}{\prod_{i=0, i\neq j}^{m-1}(j-i)} \sum_{l=0}^{m-1-k} \tilde{\sigma}_l\big(0, \dots, -(j-1)\big) \tilde{\sigma}_{m-1-k-l}\big(-(j+1), \dots, -(m-1)\big) \end{cases}$$

Ainsi :

$$\forall x \in [\![0, m-1]\!], \tilde{P}_m(Q_n)(x) = \tilde{Q}_n(x)$$

On peut étendre l'égalité à tous les entiers relatifs en restant dans le modulo m :

$$\forall x \in \mathbb{Z}, \tilde{P}_m(Q_n)(x[m]) = \tilde{Q}_n(x[m])$$

Alex R.