# PSFPN : Remontée de Hensel et reconstruction rationnelle pour la factorisation et la résolution d'équations polynomiales

Encadrant : Jérémy Berthomieu

Nombre d'étudiants : 2 ou 3.

Description : Soit $\mathbb{Z}$ l'anneau des entiers. Soit $P$ un polynôme dans $\mathbb{Z}[y]$. Le calcul des zéros de $P$ ou de la factorisation de $P$, en général, font intervenir de grands entiers ou des rationnels avec des numérateurs ou des dénominateurs qui grandissent rapidement. Afin de contrôler la taille des opérandes, il est classique de choisir des nombres premiers distincts $p_1, \ldots, p_r$ tels que leur produit majore le résultat. Le problème est alors résolu séparément modulo $p_1$,..., modulo $p_r$ puis l'on remonte la solution sur $\mathbb{Z}$ à l'aide du théorème des restes chinois.

Dans ce projet, nous proposons une alternative, appelée remontée de Hensel, qui ne fait intervenir qu'un seul nombre premier. Soit $p$ ce nombre premier. Si $P$ admet un zéro simple dans $\mathbb{Z}/p\mathbb{Z}$, alors $P$ admet un zéro dans l'ensemble des entiers $p$-adiques

$$\mathbb{Z}_p = \left\{ \sum_{k=0}^{\infty} a_k p^k,\ \forall k, 0 \leqslant a_k \leqslant p-1 \right\}.$$

Cet anneau est l'analogue des séries formelles pour les entiers en base $p$.

À partir de la solution modulo $p$, la remontée de Hensel nous permet de la calculer modulo $p^2$, puis $p^4$, $p^8$, *etc.* Lorsque $p^{2^k}$ est suffisamment grand, l'algorithme de reconstruction rationnelle nous permet de retrouver, à partir de ce développement, l'entier ou le rationnel qui annule le polynôme $P$.

Cette méthode se généralise au cas des polynômes à deux variables sur un corps ou à la factorisation de $P$ dans $\mathbb{Z}[y]$ ou $\mathbb{K}[x][y]$ avec $\mathbb{K}$ un corps.

Une implantation des ces algorithmes sera effectuée en C en utilisant en particulier la bibliothèque GMP pour la gestion des grands entiers.