PSFPN : Algorithmique pour les entiers p-adiques

Encadrant : Jérémy Berthomieu
Adresse de contact : jeremy.berthomieu@lip6.fr

Nombre d'étudiants : 2.

Description :

On souhaite s'intéresser à une méthode alternative aux restes chinois pour résoudre différents problèmes sur les entiers ou les rationnels.

Le calcul des zéros de $P \in \mathbb{Z}[x]$ ou de la factorisation de P font, en général, 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 $p_1, \ldots, p_r$ puis l'on remonte la solution sur $\mathbb{Z}$. C'est la méthode des restes chinois.

Dans ce projet, nous proposons de ne travailler qu'avec un seul nombre premier p. À partir d'une solution ou d'une factorisation modulo p, on peut alors *remonter* cette solution ou cette factorisation dans l'anneau 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 [Gat84] nous permet de la calculer modulo p^2, puis p^4, p^8, *etc.*

Comme pour le CRT, si l'on peut estimer la taille du résultat sur les entiers, alors lorsque p^{2^k} est suffisamment grand, l'algorithme de reconstruction rationnelle nous permet de retrouver, à partir de ce développement, le résultat sur les entiers ou sur les rationnels. Alors que pour le CRT, on peut se demander comment recombiner de multiples solutions modulo $p_1, \ldots, p_r$ en une ou des solutions sur $\mathbb{Z}$ ou $\mathbb{Q}$, dans le cas des entiers p-adiques, cette question n'a pas lieu d'être.

Les entiers p-adiques admettant un développement infini, nous proposons dans ce projet d'étudier comment représenter en machine de tels objets et comment calculer avec, en implantant les algorithmes en `C` [BK78].

Du point de vue applicatif, une arithmétique efficace sur les entiers p-adiques pourrait servir en cryptographie. En effet, le problème de comptage de points sur une courbe elliptique ou hyperelliptique est essentiel et l'algorithme de Kedlaya permet de le résoudre lorsque la courbe considérée est à coefficients dans un anneau d'entiers p-adiques.

Références

[BK78] Brent, R. P. and Kung, H. T., 1978. Fast algorithms for manipulating formal power series. Journal of the ACM, 25, 581–595.

[Gat84] von zur Gathen, J., 1984. Hensel and Newton methods in valuation rings. Math. Comp., 42(166), 637–661.

[Ked01] Kedlaya, K., 2001. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. J. Ramanujan Math. Soc., 16(4), 323–338..