Précision p-adique, application à la résolution d'équations différentielles

P. Lairez, **T. Vaccon**
TU Berlin, Université de Rennes 1
lairez@tu-berlin.de,tristan.vaccon@univ-rennes1.fr

24 septembre 2014

Ces deux dernières décennies ont vu une hausse de la popularité des méthodes p-adiques en calcul formel. Par exemple :

- dans [1], A.Bostan et ses co-auteurs ont utilisé des sommes de Newton pour des polynômes sur les les p-adiques afin de calculer des produits composés de polynômes sur des corps finis ;
- dans [3] P.Gaudry et ses co-auteurs ont utilisé des méthodes de relevés p-adiques pour générer des courbes hyperelliptiques de genre 2 à multiplication complexe ;
- dans [4] K.Kedlaya a utilisé une cohomologie p-adique pour compter des points sur des courbes hyperelliptiques sur des corps finis ;
- dans [5], R.Lercier et T.Sirvent calculent des isogénies entre courbes elliptiques sur des corps finis par la résolution d'équations différentielles dans $\mathbb{Z}_p$.

Cependant, de même que pour les nombres réels, la manipulation sur machine des nombres p-adiques se fait nécessairement de manière approchée, ce qui amène au problème de la gestion de la précision.

Dans [2], X.Caruso, D.Roe et moi-même proposons une manière optimale et géométrique de gérer la précision. Elle repose sur le résultat d'analyse suivant :

Lemme. *Soient E et F deux $\mathbb{Q}_p$-espaces vectoriels de dimension finie. Soit $f : E \to F$ une fonction. On suppose que f est différentiable en un certain point $v_0 \subset U$ et que la différentielle $f'(v_0)$ est surjective.*

Alors, il existe un $\delta \in \mathbb{R}_+^*$ tel que pour tout $0 \leq r \leq \delta$:

$$f(v_0 + B(0,r)) = f(v_0) + f'(v_0) \cdot B(0,r). \tag{1}$$

On peut interpréter $B(0,r)$ dans le lemme comme la donnée de précision sur l'entrée v_0 et on voit alors que la précision (optimale) sur la sortie $f(v_0)$ est donnée par $f'(v_0) \cdot B(0,r)$.

De plus, on peut effectivement déterminer un δ comme dans le lemme, via un calcul des normes des différentielles supérieures. Enfin, l'exemple du calcul de la suite SOMOS 4 montre qu'une méthode "de relevés arbitraires" permet d'atteindre la précision optimale même à travers un algorithme qui naïvement perdrait trop de précision.

Nous souhaitons présenter un travail en cours, dans lequel nous calculons la perte de précision optimale pour les équations différentielles étudiées dans [1] et [5]. Celles-ci sont de la forme $y' = g(x)h(y(x))$ avec $g, h \in \mathbb{Z}_p[[x]]$, $g(0) = h(0) = 1$, et en sachant qu'elle admet une solution $y_0 \in \mathbb{Z}_p[[x]]$. [1] et [5] montrent que connaissant g et h à précision $O(p^N)$, on connait le coefficient d'ordre n de y_0 à précision $O(p^{N-\log_p^2 n})$. Grâce à la méthode différentielle, nous montrons que la précision intrinsèque sur ce n-ème coefficient est $O(p^{N-\log_p n})$. De plus, nous donnons des bornes explicites permettant d'atteindre cette perte de précision : $N > 2\log_p n$.

Enfin, grâce à l'application de la méthode "des relevés arbitraires", nous expliquons comment atteindre cette perte de précision de manière effective et efficace par une méthode de Newton.

Cet exposé sera ainsi l'occasion, à travers l'étude de ces équations différentielles, de présenter et d'illustrer à la fois la précision différentielle en p-adique et la méthode "des relevés arbitraires".

Bibliographie

[1] A. Bostan, L. González-Vega, H. Perdry, É. Schost, *From Newton sums to coefficients : complexity issues in characteristic p*, Proceedings MEGA'05 (2005).

[2] X. Caruso, D. Roe, T. Vaccon *Tracking p-adic precision*, LMS Journal of Computation and Mathematics, volume 17, issue A, pp. 274-294.

[3] P. Gaudry, T. Houtmann, A. Weng, C. Ritzenthaler, D. Kohel, *The 2-adic CM method for genus 2*, Asiacrypt 2006, vol. 4284 of Lecture Notes in Comput. Sci. (2006), 114–129

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

[5] R. Lercier, T. Sirvent, *On Elkies subgroups of ℓ-torsion points in elliptic curves defined over a finite field*, J. Théorie des Nombres de Bordeaux **20** (2008), 783–797