# Un algorithme à la Kedlaya pour compter les points de revêtements cycliques de la droite projective

Cécile GONÇALVES

Le comptage de points de la jacobienne d'une courbe est un problème intervenant naturellement en théorie des nombres et en cryptographie.

L'algorithme proposé par Schoof [Sch85] dans les années 1980 fut le premier à effectuer cette opération en temps polynomial. Cependant, cet algorithme n'est valable qu'en petit genre.

L'algorithme proposé par Kedlaya en 2001 [Ked01] est l'un des premiers à être pratiquable en genre supérieur à 2 : c'est un algorithme qui permet de compter les points d'une courbe hyperelliptique et qui est polynomial en le genre, grâce à l'utilisation de la cohomologie de Monsky et Washnitzer. Cet algorithme est particulièrement bien adapté en petite caractéristique. Depuis, cet algorithme a été étendu à d'autres classes de courbes dont les courbes superelliptiques [GG01] et les courbes $\mathcal{C}_{a,b}$ [DV06].

Dans cet exposé, nous présenterons un algorithme à la Kedlaya de comptage de points d'un revêtement cyclique de la droite projective, qui résulte en fait d'une extension de l'algorithme proposé par P. Gaudry et N. Gürel pour les courbes superelliptiques.

## Références

[DV06] Jan Denef and Frederik Vercauteren. Counting points on $C_{ab}$ curves using Monsky-Washnitzer cohomology. *Finite Fields Appl.*, 12(1) :78–102, 2006.

[GG01] Pierrick Gaudry and Nicolas Gürel. An extension of Kedlaya's point-counting algorithm to superelliptic curves. In *Advances in cryptology—ASIACRYPT 2001 (Gold Coast)*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 480–494. Springer, Berlin, 2001.

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

[Sch85] René Schoof. Elliptic curves over finite fields and the computation of square roots mod $p$. *Math. Comp.*, 44(170) :483–494, 1985.