# Comptage de points de courbes hyperelliptiques en genre 3 et au-delà, théorie et pratique.

Simon Abelard

Le comptage de points d'une courbe algébrique définie sur un corps fini est une primitive essentielle en théorie des nombres, avec des applications en cryptographie, en géométrie arithmétique et pour les codes correcteurs. Étant donné un polynôme bivarié $F \in \mathbb{F}_{p^n}[x, y]$, il s'agit de calculer une série génératrice rationelle associée au nombre de solutions de $F(x, y) = 0$ sur $\mathbb{F}_{p^n}$, $\mathbb{F}_{p^{2n}}$, $\mathbb{F}_{p^{3n}}$, etc. Nous nous intéressons en particulier au cas des courbes hyperelliptiques (i.e. $F(x, y) = y^2 - f(x)$, avec $f$ sans facteur carré) définies sur un corps fini de grande caractéristique. Avec une complexité polynomiale en $\log p$, les algorithmes dérivés de ceux de Schoof [4] et de Pila [3] sont actuellement les plus adaptés pour ce cas de figure. Ils sont d'ailleurs utilisés en genre 1 et 2 pour construire des courbes cryptographiquement sûres. En revanche, la dépendance de leur complexité en le genre $g$ de la courbe est exponentielle, ce qui constitue un obstacle sérieux à l'emploi de ces algorithmes en genre 3 et au-delà.

Du côté théorique, nous nous sommes intéressé à cette dépendance en $g$ et nous avons proposé un algorithme de comptage de points sur des courbes hyperelliptiques dont la complexité est en $f(g)(\log q)^{O(g)}$, avec $f$ une fonction ne dépendant que de $g$, à comparer avec la borne en $(\log q)^{O(g^2)}$ établie dans [1].

L'étape essentielle des algorithmes à la Schoof-Pila consiste à obtenir une représentation efficace de la $\ell$-torsion de la jacobienne de la courbe, afin de réduire au maximum le coût des opérations dans cet espace. Pour ce faire, on décrit la $\ell$-torsion par un système polynomial dont on va ensuite calculer une résolution géométrique. La clé de voûte de notre résultat est que le système est construit de telle sorte qu'il possède naturellement une structure multihomogène qui diminue grandement la complexité d'un tel calcul.

Du côté pratique, la dépendance exponentielle se fait cruellement sentir dès le genre 3, d'où l'intérêt de commencer à étudier le cas d'une sous-famille de courbes dites à multiplication réelle, déjà traité en genre 2 dans [2]. Ces courbes sont munies d'une structure particulière qui permet essentiellement de découper la $\ell$-torsion en somme directe de trois sous-espaces plus petits, qui sont des noyaux de certains endomorphismes. On cherche alors non plus à modéliser directement la $\ell$-torsion, c'est-à-dire le noyau de la multiplication par $\ell$, mais les noyaux des endomorphismes en lesquels $\ell$ se factorise. Cela permet de diminuer fortement les degrés des systèmes polynomiaux, en ne modifiant que très légèrement la modélisation par rapport au cas général. In fine, la structure additionnelle des courbes à multiplication réelle nous permet d'obtenir un algorithme de comptage de points de complexité $\widetilde{O}((n \log p)^6)$.

Travail en commun avec Pierrick Gaudry et Pierre-Jean Spaenlehauer.

## Références


[1] L. M. Adleman and M.-D. Huang. Counting points on curves and Abelian varieties over finite fields. *Journal of Symbolic Computation*, 32(3) :171–189, 2001.

[2] P. Gaudry, D. R. Kohel, and B. A. Smith. Counting points on genus 2 curves with real multiplication. In *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 504–519. Springer, 2011.

[3] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Mathematics of Computation*, 55(192) :745–763, 1990.

[4] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44(170) :483–494, 1985.