

ATELIER « COMPTAGE DE POINTS : THÉORIE, ALGORITHMES ET PRATIQUE »  
19–23 AVRIL 2010

WORKSHOP ON COUNTING POINTS: THEORY, ALGORITHMS AND PRACTICE  
APRIL 19–23, 2010

## Fast $p$ -adic arithmetic for (hyper)elliptic AGM point counting algorithms

Reynald Lercier

Institut de Recherche Mathématiques de Rennes (IRMAR)  
DGA & Université de Rennes 1  
Campus Beaulieu, 263 avenue du Général Leclerc  
35042 Rennes Cedex  
FRANCE

reynald.lercier@m4x.org

---

In 2002, Mestre proposed a very efficient  $p$ -adic method for counting points on elliptic and hyperelliptic curves in  $\text{GF}(2^n)$ . In this talk, we present a survey of the numerous algorithmic improvements, due to Satoh–Skjernaa–Taguchi, Gaudry, Kim *et al.*, Lercier–Lubicz, Harley, etc. . . which made decrease the complexity in time to  $O(n^{2+o(1)})$ . Especially, we focus on the choice of good basis for  $p$ -adic unramified extensions, a central point in these ideas, and compare with the use of normal elliptic basis introduced by Couveignes and Lercier in 2009.