

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

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

Genus 1 point counting in essentially quartic time and quadratic space

Andrew V. Sutherland

Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
USA

drew@math.mit.edu

The time and space complexity of the most efficient point-counting algorithms for genus 1 curves over finite fields of large characteristic is dominated by the task of computing and evaluating modular polynomials. With the fast algorithms now available the limiting factor is space, not time. The common practice of using precomputed modular polynomials has a space requirement that is quartic in $\log(q)$, where q is the size of the field. If one computes modular polynomials as required (and then discards them), the space complexity is quasi-cubic. I will present an algorithm that simultaneously computes and evaluates a modular polynomial over a prime field using quasi-quadratic space, with a quasi-cubic time complexity that is as good as (and practically faster than) existing algorithms for computing modular polynomials.

When used in conjunction with the SEA algorithm, this allows one to count the points on a genus 1 curve over a prime field in quasi-quartic time and quasi-quadratic space. In practical terms, the proposed algorithm can handle modular polynomials of level as high as 30,000 for the j -function, and over 100,000 when more favorable modular functions are used.