Efficient Point-Counting Algorithms for Superelliptic Curves via the Cartier Operator and the Hasse-Weil Bound

Hase-Liu, Matthew (School: Highland Park High School)

Purpose: Given a prime p and polynomial f, how many pairs (x,y) are there such that y^a-x^b*f(x) is a multiple of p? Equivalently, how many rational points lie on a superelliptic curve? Answering these questions has salient applications in developing Jacobian-based cryptosystems (an extension of elliptic curve cryptosystems), creating Goppa codes for error correction, and generating experimental data for generalizations of the Sato-Tate conjecture. Problem and Hypothesis: Does there exist a fast point-counting algorithm for superelliptic curves? We hypothesize that methods for hyperelliptic curves can be generalized to the case of superelliptic curves with similar runtimes. Approach: Under a few constraints, the Hasse-Weil bound ensures that the number of points modulo p uniquely determines the actual number of points (#C(F_p)) on a curve C over the finite field F_p. To compute #C(F_p) mod p, we use a powerful congruence relating #C(F_p) to the trace of the Hasse-Witt matrix of C, whose entries we express in terms of multinomial coefficients. For the specific family of trinomial superelliptic curves, these multinomial coefficients are actually binomial coefficients, which we can simplify modulo p by solving the computationally easier problem of quadratic Diophantine equations. Results: Our methods are asymptotically the most efficient known point-counting algorithms for families of trinomial superelliptic curves; while a naive brute-force algorithm has a quadratic runtime, our method runs in polylogarithmic time, limited only by the simplification of the binomial coefficients. Future Work: We plan to implement our algorithms for calculating the order of the Jacobian group of C and extend our point-counting approach to all general trinomial curves.

Awards Won:

American Mathematical Society: Second Award of $1,000

Third Award of $1,000