Constructing genus 2 curves over finite fields.

Kirsten Eisentraeger, Pennsylvania State

We present an algorithm for constructing genus 2 curves over a finite field with a given number of points on its Jacobian. This has important applications in cryptography, where groups of prime order are used as the basis for discrete-log based cryptosystems. For a quartic CM field K with primitive CM type, we compute the Igusa class polynomials modulo p for certain small primes p and then use the Chinese remainder theorem and a bound on the denominators to construct the class polynomials. We will also discuss some improvements to this.