Speaker: Travis Morrison
Title: Computing supersingular endomorphism rings with inseparable endomorphisms

Abstract. Given an algorithm for computing random endomorphisms of a supersingular elliptic curve E, how many calls to that algorithm are required to find a generating set for the endomorphism ring of E? We will discuss an algorithm for computing an inseparable endomorphism of E. Two calls to this algorithm provably produces a basis for a Bass suborder of the endomorphism ring of E. We will conclude with a heuristic argument that the expected number of calls to this algorithm to generate the full endomorphism ring is bounded by a constant — experimental data suggests this expectation is between 3 and 4.