Speaker: Andrew Sutherland

Title: Genus 1 point counting in quadratic space and essentially quartic time

Abstract: The Schoof-Elkies-Atkin (SEA) algorithm is the method of choice for counting points on an elliptic curve modulo a prime p. Its main limitation is the size of the modular polynomials it requires. The largest of these uses on the order of $n^3 \log n$ bits of storage, where $n = \log p$, and their aggregate size is quartic in n.

I will describe a modified version of the SEA algorithm that requires only quadratic space. This is based on a new technique for directly computing partially instantiated modular polynomials (and their derivatives), using isogeny volcanoes and an explicit form of the Chinese remainder theorem. The resulting algorithm is not only able to handle much larger problem sizes, its reduced space complexity also yields a better running time. This work has enabled a new point counting record, modulo a prime p with over 5000 decimal digits – more than doubling the previous record of 2500 digits.

Time permitting, I will also discuss how these techniques may be used to reduce the space complexity of some other problems in computational number theory.