Algebra Seminar

Counting Problems for Elliptic Curves over a Fixed Finite Field

Nathan Kaplan
UC Irvine

Abstract: Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Hasses theorem says that $\#E(\mathbb{F}_q) = q + 1 - t_E$ where $|t_E| \leq 2\sqrt{q}$. Deuring uses the theory of complex multiplication to express the number of isomorphism classes of curves with a fixed value of t_E in terms of sums of ideal class numbers of orders in quadratic imaginary fields. Birch shows that as q goes to infinity the normalized values of these point counts converge to the Sato-Tate distribution by applying the Selberg Trace Formula.

In this talk we discuss finer counting questions for elliptic curves over $\mathbb{F}_q$. For example, what is the probability that the number of rational points is divisible by 5? What is the probability that the group of rational points is cyclic? If we choose a curve at random, and then pick a random point on that curve, what is the probability that the order of the point is odd? We study the distribution of rational point counts for elliptic curves containing a specified subgroup, giving exact formulas for moments in terms of traces of Hecke operators. We will also discuss some open problems. This is joint with work Ian Petrow (ETH Zurich).

Tuesday, March 27, 2018, 4:00 pm
Mathematics and Science Center: W304

Mathematics and Computer Science
Emory University