Algebra Seminar

Hyperelliptic curves, L-polynomials, and random matrices

Andrew Sutherland
Massachusetts Institute of Technology

Abstract: For a smooth projective curve C/Q, the zeta function $Z(C/F_p;T)$ is a rational function whose numerator $L_p(T)$ encodes arithmetic data attached to the curve. We consider the distribution of normalized L-polynomials of C as p varies over primes where C has good reduction. For a typical hyperelliptic curve of genus g, the Katz-Sarnak model implies that this distribution matches the distribution of characteristic polynomials of random matrices in the unitary symplectic group $USp(2g)$, which may be viewed as a generalization of the Sato-Tate conjecture. But there are many atypical cases: in genus 2 we already find 27 exceptional distributions. I will describe the large scale numerical experiments (involving more than 10 billion curves) that eventually led to a theoretical model that explains all of the exceptional distributions that have been observed in genus 2, and predicts that there are no others. Some key computational tools include: fast group operations in the Jacobian (borrowed from cryptography), and a method to quickly classify unknown distributions by approximating their moment sequences. This is joint work with Kiran Kedlaya.

Tuesday, February 15, 2011, 3:00 pm
Mathematics and Science Center: W306

Mathematics and Computer Science
Emory University