Algebra Seminar

Constructing Picard curves with complex multiplication using the Chinese Remainder Theorem

Sonny Arora
Emory University

Abstract: For cryptographic protocols whose security relies on the di?culty of the discrete log problem of the underlying group, one often wants to ?nd a group whose order is divisible by a large prime. One option for the group is the group of points of an elliptic curve over a ?nite ?eld, or more generally, the group of points on the Jacobian of a curve over a ?nite ?eld. To find curves over a finite field whose Jacobian has number of points divisible by a large prime, it suffices to construct curves whose Jacobian is ordinary and has complex multiplication (CM) by a given field K. Working with higher genus curves allows one to work over smaller fields than the elliptic curve case. I will present a new algorithm to construct a particular class of genus 3 curves, called Picard curves, whose Jacobian is ordinary with CM by a given field CM field K. This is joint work with Kirsten Eisentraeger.

Tuesday, April 16, 2019, 4:00 pm
Mathematics and Science Center: W201

Mathematics
Emory University