Number Theory Seminar

The distribution in arithmetic progressions of primes of cyclic reduction for elliptic curves

John Sung Min Lee (University of Illinois at Chicago)

Abstract: Given an elliptic curve $E/\mathbb{Q}$ and a prime $p$ of good reduction for $E$, let $\tilde{E}_p$ denote the reduction of $E$ modulo $p$. If $\tilde{E}_p(\mathbb{F}_p)$ forms a cyclic group, we call $p$ a prime of cyclic reduction for $E$. In this talk, we study the issue of which arithmetic progressions $k \pmod{n}$ have the property that, for all but finitely many primes $p \equiv k \pmod{n}$, the group $\tilde{E}_p(\mathbb{F}_p)$ is not cyclic, answering a question of Akbal and G"{u}lo"{u}lu. Also, we show that primes of cyclic reduction are statistically biased modulo $n$, refining Banks and Shparlinski's results on average density of primes of cyclic reduction. The first part of this talk is a joint work with Nathan Jones.

Friday, September 15 at 1:00 PM in 427 SEO