LILJANA BABINKOSTOVA, Boise State University

Elliptic Pseudoprimes

Efficiently distinguishing prime and composite numbers is one of the fundamental problems in number theory. In 1987, Gordon introduced analogues of Fermat pseudoprimes and Carmichael numbers for elliptic curves with complex multiplication (CM): elliptic pseudoprimes, strong elliptic pseudoprimes and elliptic Carmichael numbers.

Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by an order in $\mathbb{Q}(\sqrt{-d})$ and let $P \in E(\mathbb{Q})$ have infinite order. A composite number N is called an elliptic pseudoprime if $(\frac{-d}{N}) = -1$, N is coprime to $\Delta(E)$, and N satisfies $(N+1)P \equiv \mathcal{O} \pmod{N}$.

In 2012, Silverman extended Gordon's notion of elliptic pseudoprimes and elliptic Carmichael numbers to arbitrary elliptic curves.

Let $N \in \mathbb{Z}$, let $E/\mathbb{Q}$ be an elliptic curve, and let $P \in E(\mathbb{Z}/N\mathbb{Z})$. Write the L-series of $E/\mathbb{Q}$ as $L(E/\mathbb{Q}, s) = \sum_n \frac{a_n}{n^s}$. Then N is an elliptic pseudoprime for (E, P) if N has at least two distinct prime factors, E has good reduction at every prime p dividing N, and $(N+1-a_N)P \equiv \mathcal{O} \pmod{N}$.

In this talk we present results that provide bounds on the number of points on a given elliptic curve for which an odd integer N is a strong elliptic pseudoprime and probabilistic results for a given odd integer N being a strong elliptic pseudoprime for a randomly chosen point on a randomly chosen elliptic curve. In addition, we present similar results for strong elliptic pseudoprimes.