Number Theory Seminar

On Average Congruence Class Biases for Cyclicity and Koblitz problem

By

Sung Min Lee
(DAKOTA STATE UNIVERSITY)

Abstract: For an elliptic curve $E/\mathbb{Q}$ and a good prime p, $\widetilde{E}_p$ denotes the reduction of E modulo p. We call p a prime of cyclic reduction if $\widetilde{E}_p(\mathbb{F}_p)$ is cyclic, and of Koblitz reduction if the group has a prime order. Determining the asymptotics of the counting functions for these primes are known as cyclicity problem and Koblitz problem, respectively. The former was proven by J.-P. Serre under the Generalized Riemann Hypothesis, while the latter remains open. Recent work has proven both problems unconditionally ``on average,'' and Jones, assuming an affirmative answer to Serre's uniformity question, showed that the average of conjectured asymptotics align with the average results. In this talk, we first propose Koblitz problem for primes in arithmetic progressions, building upon Zywina's argument. Then, adapting Jones's methods, we refine his results by removing the assumption and restricting primes to lie in arithmetic progressions. Additionally, we present a rather counterintuitive observation that primes of cyclic reduction and Koblitz reduction are statistically oppositely biased over congruence classes, despite the fact that primes of Koblitz reduction must also be primes of cyclic reduction. This work is a joint research with Jacob Mayle and Tian Wang.

Date: Thursday, October 24, 2024
Time: 18:00
Place: ZOOM

To request the event link, please send a message to guloglua@fen.bilkent.edu.tr