Numerical Analysis and Scientific Computing Seminar

Minimal and nilpotent images of Galois for elliptic curves

Jeremy Rouse
Wake Forest University

Abstract: If K is a number field and E/K an elliptic curve, then for every positive integer n, there is a Galois representation $\rho_{E,n} : G_K \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. If $K = \mathbb{Q}$, $\det \circ \rho_{E,n} : G_{\mathbb{Q}} \to (\mathbb{Z}/n\mathbb{Z})^\times$ is surjective. We say that a subgroup H of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is *minimal* if $\det : H \to (\mathbb{Z}/n\mathbb{Z})^\times$ is surjective. We show that essentially the only way for the image of $\rho_{E,n}$ to be minimal is for n to be a power of 2, and that minimal subgroups of $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ are plentiful.

The question of minimality is connected with the question of when the Galois group of $\mathbb{Q}(E[n])/\mathbb{Q}$ is a nilpotent group. In 2016, Lozano-Robledo and González-Jiménez showed that if $E/\mathbb{Q}$ is an elliptic curve and $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is abelian, then $n \in \{2, 3, 4, 6, 8\}$. We show that, subject to a positive answer to Serre's uniformity question, if $E/\mathbb{Q}$ is a non-CM elliptic curve and $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is nilpotent, then $n \in \{2^k, 3, 5, 6, 7, 15, 21\}$.

All of the work in this talk is joint with Harris Daniels.

Tuesday, February 25, 2025, 4:00 pm
Mathematics and Science Center: MSC W301

Mathematics
Emory University