Contribution ID: **12** Type: **not specified**

Spectral theory of isogeny graphs

Wednesday, 20 September 2023 14:30 (1 hour)

A familiar object in isogeny based cryptography is the graph whose vertices are supersingular elliptic curves and whose edges are isogenies of fixed degree ℓ. It is immediate to prove that from each vertex there are exactly $\ell+1$ outgoing edges, while it is less obvious that such a graph is connected and that it has the Ramanujan property, a property about the spectrum of the adjacency matrix implying that random walks very soon visit all vertices with the same probability. In our talk we look at a generalization of these graphs, namely graphs whose vertices are pairs (E,T), where E is a supersingular elliptic curve and T is some information on the n-torsion of E (e.g. a basis, a point, a subgroup) for fixed n. These graphs can be multipartite, implying that the Ramanujan property is not always satisfied. By studying modular curves over mixed characteristic we relate isogeny graphs to geometric and cohomological objects, which allows us to prove the appropriate modification of the Ramanujan property.

Primary author: LIDO, Guido Maria (Roma Tor Vergata)

Co-author: CODOGNI, Giulio (Roma Tor Vergata)

Presenter: LIDO, Guido Maria (Roma Tor Vergata)