Sarah Arpin (Universiteit Leiden)

Title: Orienteering with one endomorphism

Abstract: In joint work with M. Chen, K. Lauter, R. Scheidler, K. Stange, and H. Tran, we provide algorithms for finding paths between supersingular elliptic curves via the information of one endomorphism of the input curve. In particular, we use the volcano structure of the oriented supersingular isogeny graph to take ascending/descending/horizontal steps on the graph and deduce path-finding algorithms to an initial curve. Each altitude of the volcano corresponds to a unique quadratic order, called the primitive order. We introduce a new hard problem of computing the primitive order given an arbitrary endomorphism on the curve, and we also provide a sub-exponential quantum algorithm for solving it.

Jef Laga (Princeton University)

Title: Rational torsion on abelian surfaces with quaternionic multiplication

Abstract: Mazur classified all possible rational torsion subgroups of elliptic curves over Q. In joint work with Ciaran Schembri, Ari Shnidman and John Voight, we put strong constraints on the torsion subgroup of a class of abelian surfaces whose geometric endomorphism algebra is large, namely an indefinite quaternion algebra.

Ross Paterson (University of Bristol)

Title: Quadratic Twists as Random Variables

Abstract: If E/Q is an elliptic curve, and d is a squarefree integer, then the 2-torsion modules of E and its quadratic twist E_d are isomorphic. In particular their 2-Selmer groups lie in the same space. Poonen-Rains provide a heuristic model for the behaviour of these 2-Selmer groups individually, as E varies, but how independent are they? We'll present results in this direction.

Caleb Springer (University College London)

Title: Abelian varieties and their groups of rational points

Abstract: There has been a recent flurry of research activity concerning the groups of rational points of abelian varieties defined over finite fields. One productive perspective involves describing the group of rational points as a module over the endomorphism ring. In the case of elliptic curves, this module structure was completely described by Lenstra. I continue the story for abelian varieties of higher dimension, along with Stefano Marseglia, and we present several interesting consequences.