AMIR AKBARY-MAJDABADNO, University of Lethbridge

On invariants of elliptic curves on average

For an elliptic curve E defined over $\mathbb{Q}$ and a prime p of good reduction, it is known that the group of rational points $E_p(\mathbb{F}_p)$ of the reduction mod p of E over the finite field $\mathbb{F}_p$ is the product of at most two cyclic groups. Let $i_E(p)$ be the index of the largest cyclic subgroup of $E_p(\mathbb{F}_p)$. We describe a general theorem regarding certain functions of $i_E(p)$ on average over the family of all elliptic curves inside a box. We derive several results related to some invariants of elliptic curves as corollaries to this general theorem. This is a joint work with Adam Felix (KTH, Sweden).