Elliptic curves with prescribed groups over finite fields and the Cohen-Lenstra Heuristics

Chantal David, Concordia University

Let $G_{m,k} := \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$ be an abelian group of rank 2 and order $N = m^2 k$. When does there exist a finite field $\mathbb{F}_p$ and an elliptic curve $E/\mathbb{F}_p$ such that $E(\mathbb{F}_p) \simeq G_{m,k}$? We show that this happens with probability 0 when k is very small with respect to m, and with probability 1 when k is big enough with respect to m. The fact that the groups $G_{m,k}$ are more likely to occur when k is big is reminiscent of the Cohen-Lenstra heuristics which predict that a random abelian group G occurs with probability weighted by $\#G/\#\mathrm{Aut}(G)$. By counting the average number of times that a given group $G_{m,k}$ occurs over the finite fields $\mathbb{F}_p$ (and not simply if a given group occurs or not), we are able to verify that the probability of occurrence of the groups $G_{m,k}$ is indeed weighted by the Cohen-Lenstra weights.

This is joint work with V. Chandee, D. Koukoulopoulos and E. Smith.