Counting points on modular curves

Andrew Sutherland
Massachusetts Institute of Technology, USA
drew@math.mit.edu

Let H be an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, let X_H be the corresponding modular curve that parametrizes elliptic curves with H-level structure, and let $\mathbb{F}_q$ be a finite field whose characteristic does not divide the level of H.

I will discuss improvements to the moduli-theoretic approach for computing $\#X_H(\mathbb{F}_q)$ that lead to an algorithm that is practically and asymptotically faster than existing approaches as q, the genus of X_H, and the level of H vary.