Queen's Algebraic Geometry — Seminar —

On the order of a rational point of an elliptic curve (mod p)

AMIR AKBARY
University of Lethbridge

Abstract

Let E be an elliptic curve defined over $\mathbb{Q}$. For any prime p of good reduction, let E_p be the elliptic curve over the finite field $\mathbb{F}_p$ obtained by reducing E modulo p. We investigate that for a point of infinite order in the Mordell group $E(\mathbb{Q})$, how the order of the reduction of this point mod p varies as p goes to infinity. We study this problem by comparison with reduction of integers mod p. We also describe some of our recent work (joint with Kumar Murty, University of Toronto) on this topic.

Monday, February 5, 2007
4:30pm – 5:30pm
115 Jeffery Hall