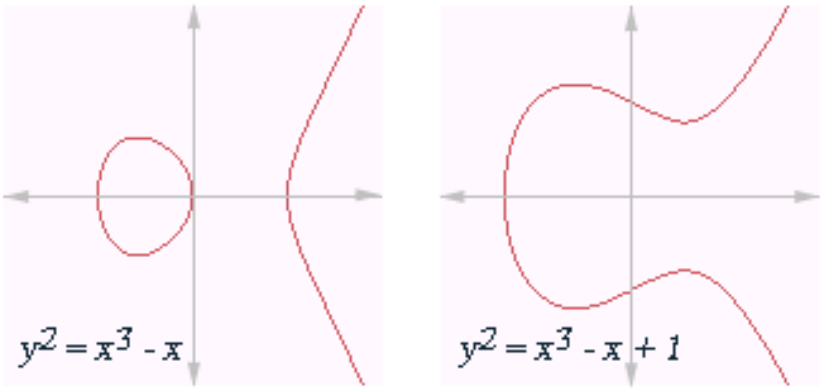
Endomorphism Rings of Elliptic Curves

Wednesday, January 30
4:00-5:XX pm, TSC 211

Stefan Erickson
Colorado College

Rated PG-13 (Background in Abstract Algebra)



Abstract

Elliptic curves are an essential tool in number theory. Andrew Wiles's proof of Fermat's Last Theorem showed that semistable elliptic curves are modular. The Birch Swinnerton-Dyer Conjecture, which relates the rank of elliptic curve group over Q and the order of vanishing of its associated L-function, is one of the seven Millenium problems. Elliptic curves over finite fields are the basis for modern cryptosystems.

One important invariant of an elliptic curve is its ring of endomorphisms. The existence of "extra" endomorphisms often times make certain proofs simpler (or even possible) and creates both destructive and constructive applications in elliptic curve cryptography.

After a brief introduction to elliptic curves, we will investigate the properties of their endomorphism rings. We will delve into complex multiplication and explain why elliptic curves can be thought of as complex tori. We will conclude with a surprising simple classification of all such endomorphism rings for elliptic curves defined over the complex numbers and over finite fields.