

CO 690: Elliptic Curves

Winter 2007

Instructor: David Jao, djao@math.uwaterloo.ca, MC 5038, x32493.

Course web page: <http://www.math.uwaterloo.ca/~djao/co690.2007/>

Description: This course is a semester long graduate level reading course on elliptic curves, with emphasis on arithmetic and number theoretic topics. The textbook for the course is Joseph Silverman's "Arithmetic of Elliptic Curves." Topics include the Riemann-Roch theorem, group law, isogenies, endomorphisms, Weil pairing, Tate modules, curves over local and finite fields, and (time permitting) the relationship between elliptic and modular curves.

The following chapters in the textbook will be covered:

- *Chapter I, Algebraic Varieties:* Foundations of algebraic geometry, algebra-geometry correspondence.
- *Chapter II, Algebraic curves:* Differentials, Riemann-Roch theorem, Hurwitz genus formula.
- *Chapter III, The Geometry of Elliptic Curves:* Group law, isogenies, Tate module, Weil pairing, structure of endomorphisms and automorphisms.
- *Chapter V, Elliptic Curves over Finite Fields:* Hasse-Weil bound, Weil conjectures, super-singular curves.
- *Chapter VI, Elliptic Curves over \mathbb{C} :* Elliptic functions, analytic-algebraic correspondence, complex uniformization.
- (time permitting) *Appendix C:* Complex multiplication, modular functions, modular curves.

Prerequisites: A background in abstract algebra is required. Knowledge of complex analysis or algebraic geometry is helpful; practically speaking, prior experience with at least one of the latter two subjects is required.

Evaluation: Participants will give weekly lectures on in-depth topics that complement and reinforce the reading material. Evaluations will be based on the weekly lectures. Written lecture notes for each lecture will be available online on the course web page.