

# Math 788E, Arithmetic of Elliptic Curves

Fall 2008

- **Instructor:** Matthew Boylan
- **Course Description:**

An elliptic curve over the rational numbers is an equation  $y^2 = P(x)$ , where  $P(x)$  is monic, degree 3, and has distinct roots. The points on this curve (in particular, the points with rational coordinates) form a finitely generated abelian group (this is the famous theorem of Mordell-Weil), whose torsion structure (points with finite order) is well-understood (by work of Mazur), but whose free abelian part is mysterious (the deepest questions here are captured by the Birch and Swinnerton-Dyer Conjecture, one of the Clay Math Institute's 7 Millennium problems). Moreover, many interesting problems in mathematics may be recast in the setting of elliptic curves. Examples include Fermat's Last Theorem (which requires a certain correspondence between elliptic curves and modular forms) and the congruent number problem (solved by Tunnell in the early 1980's).

I intend for this course to be an introduction to the subject.

## Here is a tentative list of topics to be covered:

- Cubic curves: Weierstrass form, discriminant,  $j$ -invariant, group law.
- Mordell-Weil Theorem: the group of rational points on an elliptic curve is abelian and finitely generated; torsion subgroup and rank of free part; heights and descent.
- Complex points: analytic isomorphism between lattices and cubic curves; elliptic functions.
- reduction modulo primes  $p$ ;  $L$ -functions of elliptic curves.
- (time permitting) discussion of Birch and Swinnerton-Dyer Conjecture; relationship of elliptic curves to Fermat's Last Theorem (including Taniyama-Shimura Conjecture) and to congruent number problem.
- **Text:**

Knapp, Anthony W. Elliptic Curves. Mathematical Notes, 40. Princeton University Press, Princeton, NJ, 1992. xvi+427 pp.
- **Other References:**
  - (1) Cassels, J. W. S. Lectures on Elliptic Curves.
  - (2) Darmon, Rational Points on Modular Elliptic Curves.
  - (3) Husemöller, Dale. Elliptic Curves.
  - (4) Silverman, Joseph H. The Arithmetic of Elliptic Curves.
  - (5) Silverman, Joseph H. Advanced Topics in the Arithmetic of Elliptic Curves.
  - (6) Silverman, Joseph H.; Tate, John. Rational Points on Elliptic Curves.
- **Homework:** Homework will be assigned weekly or once every two weeks.
- **Grading:** Grading will be based on homework. A mid-term and final exam will be administered in formats to be determined.