# Math 766: Elliptic Curves

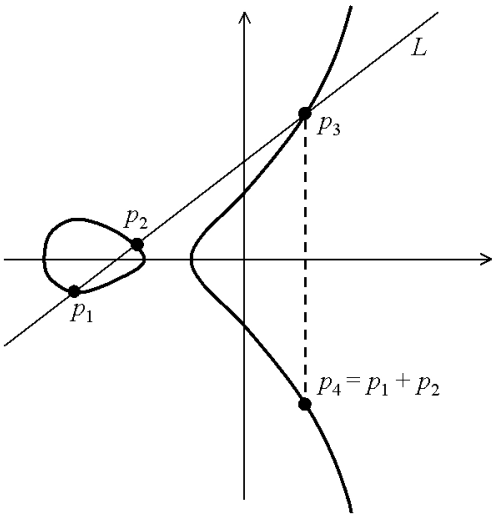
**Spring 2014 Course Information and Syllabus**
**Nathan Kaplan, DL 418,** nathan.kaplan@yale.edu

**Lectures: Tu, Th 11:35 - 1:00 in DL 431.**

## Course Goals

This course is an introduction to the arithmetic theory of elliptic curves. These curves are right on the boundary between what we understand well and what currently seems out of reach. They have played a central role in number theory and algebraic geometry over the past century and are the subject of many famous unsolved problems including the Birch and Swinnerton-Dyer Conjecture. A major goal of this course is to give a proof of the Mordell-Weil theorem, which states that for an elliptic curve defined over a number field the set of rational points forms a finitely generated abelian group. We will focus on studying this group of rational points, particularly when the curve is defined over the rational numbers. We can give a very concrete description of an elliptic curve over the rationals as the set of solution of $y^2 = x^3 + ax + b$ for rational numbers a, b. In this course we will work with many examples and see how to use the computer algebra system SAGE to better understand these curves.

Students should be familiar with Galois theory. Some familiarity with basic algebraic number theory and the p-adic numbers would also be helpful, as would some previous experience with basic algebraic geometry, particularly with algebraic curves. While this is a graduate course, it may also be appropriate for advanced undergraduates.



## Grading

For undergraduates taking this course for a grade, there will be several homework assignments throughout the semester. You are encouraged to work together on these. Undergraduates will also be required to write a final paper of 5-10 pages in length and give an in-class presentation.

### Resources

1. *The Arithmetic of Elliptic Curves*, J. Silverman. 2nd Edition
   ISBN: 978-0-387-09493-9
   This will be the primary textbook for the course.

2. *Lectures on Elliptic Curves*, J.W.S. Cassels.
   ISBN: 0-521-42530-1.

3. Andrew Sutherland's course notes for Elliptic Curves at MIT
   `http://math.mit.edu/classes/18.783/lectures.html`