

# Math 497A: Elliptic Curves and Applications to Cryptography - Fall 2008

Mo, We, Th, Fri 1:25-2:15pm, 113 McAllister

## General Information

**Instructor:** Dr. Kirsten Eisenträger

**Office:** 422 McAllister Building

**Office Phone:** (814) 863-4127

**Office hours:** We 2:15-3:00pm, Th 5:00-5:45pm, and by appointment

**Textbook:** *Rational Points on Elliptic Curves* by Joseph H. Silverman and John Tate, Springer, 1992

**Teaching Assistant:** Van Cyr, cyr at math.psu.edu, 432 McAllister Building

**Course webpage:** <http://www.math.psu.edu/eisentra/courses/math497A>

**Course Topics:** The study of diophantine equations is an area of number theory that deals with finding solutions to polynomial equations. Looking for solutions of equations in integers or rational numbers has a long history that goes back to ancient Greece. In this class we will focus on elliptic curves, a special class of diophantine equations given by certain cubic equations in two variables. We will study these equations through a combination of techniques from number theory and algebraic geometry.

We will cover the group law for elliptic curves, both in terms of the geometry of the curve and in terms of explicit equations. Then we will discuss points of finite order and isogenies. We will also study elliptic curves over the rationals and prove the Mordell-Weil theorem, which says that the group of rational points on an elliptic curve is finitely generated. After that, we will talk about elliptic curves defined over finite fields. Elliptic curves over finite fields have many applications to cryptography, and we will discuss their use in discrete-log based cryptosystems and in applications of the Weil and Tate pairings.

For the first part of the course, the first 5 chapters of Silverman-Tate will be most relevant. For the second part that deals with cryptographic applications there is no single reference. I will hand out some notes and relevant papers.

## Homework:

There will be weekly homework assignments which will be collected and graded. Homework is due at the beginning of class on the given due date (usually Friday). No late homework will be accepted without approval from the instructor in advance. You are encouraged to discuss the homework assignments with other students in the class; however, if you do, you should write on your homework submission the students with whom you discussed the assignment. You are required to write up your own solutions.

## Examinations:

There will be one 2 hour midterm in this class. The midterm will be on **Wednesday, October 8**. Each student will also take an individual oral final exam. This will be given during the period of **December 12–17**.