Math 168: Topics in Applied Math & Comp. Sci. (Fall 2005):

Explicit Approaches to Elliptic Curves and Modular Forms

Course: MW 3:00-4:20 in 201 Center
Section: Th 5:00pm in 207 Center

William Stein (wstein@ucsd.edu)
http://modular.ucsd.edu/168

Abstract

This course is an introduction to elliptic curve and modular forms, with a special emphasis on how to compute with these objects.

1 Textbooks

The main text are the notes that I've written and will be handing out. There are also many books and articles on elliptic curves and modular forms, which I will encourage you to look at. For the first quarter of the course, I will closely follow Chapter 6 of `http://modular.ucsd.edu/ent/`.

2 Course Topics

- [**Elliptic Curves**] I will define elliptic curves, explain their two main applications to cryptography, and discuss the Birch and Swinnerton-Dyer conjecture (a million dollar Clay Math prize problem).
- [**Modular Forms**] I will define modular forms of weight 2, discuss their connection with elliptic curves and Andrew Wiles's celebrated proof of Fermat's Last Theorem. I will also discuss how to use modular symbols to compute modular forms, and mention open problems.

See the course outline below for more details.

3 Prerequisites

- A course on groups, rings and fields.
- Ability to follow nontrivial mathematical arguments.
- Know how to use a computer.

It will be useful if you know something about algebraic curves, complex analysis and have some prior exposure to number theory. However, I am not requiring this as a prerequisite. A few times during the course I will give motivation for a topic or a deeper explanation for something that assume more background; I will make it clear when I am doing this, and it will not be a problem if you don't understand it.

4 Grade

Your grade will be determined as follows:

- 20% midterm
- 25% final exam
- 25% final project
- 30% homework

If you get 90% of points you'll get at least an A-, 80% will give you at least a B-, and 70% at least a C-.

5 Homework

There will be one homework assignment per week. It will be assigned by Wednesday, and be due the following Wednesday. Though I will not accept late homework, your lowest homework grade will be dropped.

Please *do* work together on homework problems!

BUT, write up your solutions individually, and carefully acknowledge the people and other sources that you used.

6 Office Hours

My office is AP&M 5111. Please come by and chat with me anytime I'm there. My official office hours will be announced later.

7 Course Outline

1. Overview of elliptic curves and modular forms
2. How to put a natural group structure on the set of points on an elliptic curve
3. Elliptic curves over finite fields
4. How to factor integers using elliptic curves (Application: cracking the RSA cryptosystems.)
5. How to make cryptosystems using elliptic curves (Application: the best public-key crypotosystems?)
6. Elliptic curves over the rational numbers
7. The group $\mathrm{SL}_2(\mathbf{Z})$ and the complex upper half plane (Ch. 7 of Serre's *A course in arithmetic*).
8. Modular curves as quotients of the upper half plane
9. What does it mean for an elliptic curve to be "modular"? (What exactly was Andrew Wiles contribution to the proof of Fermat?)
10. Introduction to modular symbols (very explicit and easy "homology" of modular curves)
11. How to use modular symbols to compute modular forms, I
12. How to use modular symbols to compute modular forms, II
13. SAGE: System for Algebra and Geometry Experimentation (on the architecture and design of SAGE).
14. The L-series of an elliptic curve over $\mathbf{Q}$
15. The Birch and Swinnerton-Dyer conjecture (a million dollar prize problem)