Math 203b, Topics in Number Theory: Elliptic Curves
Brandeis University, Fall 2014

http://people.brandeis.edu/~cwe/203b_2014/index.html

Course Summary

Instructor:	Carl Wang Erickson, cwe@brandeis.edu
Office:	Goldsmith 206
Meeting Location:	Goldsmith 226
First meeting time:	Friday August 29, 11:00AM-12:20PM
Expected meeting schedule:	Tuesday/Friday, 11:00AM-12:20PM (Block H)

Participation

Students interested in attending should register for the course. Each student will give a 45-minute presentation on some topic in the course. The timing and possible topics will be discussed once I have surveyed the background and interests of the students attending the course. **If you are interested in the course but cannot attend the first meeting, please email me.**

Undergraduate students interested in the course should also come to see me and discuss the course at the beginning of the semester.

Prerequisites: Familiarity with Galois theory and p-adic numbers will be assumed. Other advantageous topics to be familiar with include algebraic curves and basic algebraic number theory. However, the beginning of the course will introduce basic algebraic geometry according to the background of people attending the course. You are encouraged to check in with me regarding questions of background knowledge.

Course Description

The study of elliptic curves allows for an especially wide variety of techniques to be applied toward interesting results and computations – you can see many of them named in the outline below. For now, we will give an overview of this description. I would like to recognize Tom Fisher for his excellent course on elliptic curves, which is a model for this one. Our goal is to study the rational points on elliptic curves, and the perspective of his course has been a major influence.

We will start out with algebro-geometric background necessary to define elliptic curves and maps between them. We will then proceed through the main number-theoretic content of the course: the points on elliptic curves defined over various fields – finite fields, p-adic local fields, and number fields. One of the main goals is to prove the Mordell-Weil theorem, showing that the points of an elliptic curve over a number field have a nice structure. Then, we will do some calculations with rank. Throughout these studies, explicit examples and computations are readily available, and we will often explore them.

With what time is left, we may explore further topics, such as modular forms and the modularity of elliptic curves; or the Birch and Swinnerton-Dyer conjecture.

Resources

The following books are recommended for consultation and are on reserve in the library:

- Silverman, *The Arithmetic of Elliptic Curves*
- Cassels, *Lectures on Elliptic Curves*
- Silverman and Tate, *Rational Points on Elliptic Curves*

Tentative Course Outline

Motivation and Geometric Background: We will begin by giving motivation from the "congruent number problem," showing how elliptic curves appear in an ancient number theory problem. Then give some background in basic algebraic geometry in order to define an elliptic curve. This background will be customized toward the background knowledge of the students in the class. In particular, no background in algebraic geometry will be assumed, and scheme theory, while helpful for those who are familiar with it, will not be used. From this background, we will be able to discuss the equations defining elliptic curves and describe how an elliptic curve is a group variety. We will then study of isogenies between elliptic curves and differentials on them.

Potential Talks: Elliptic curves over $\mathbb{C}$ and the Weierstrass $\wp$-function; Algebraic curves

Elliptic Curves over Finite Fields: We will be able to apply the geometric background to the Frobenius morphism, resulting in a bound on the number of points on an elliptic curve with coordinates in a finite field.

Potential Talks: Supersingular and ordinary elliptic curves

Elliptic Curves over Local Fields: In studying elliptic curves over p-adic fields, we will use our knowledge over finite fields and the notion of a formal group in order to construct and understand a filtration on the points of the curve. Adic topologies and formal groups will be thouroughly discussed, as well as good and bad reduction types.

Potential Talks: Tamagawa numbers, local L-factors.

Elliptic Curves over Global Fields: Points The points of elliptic curves over number fields is our main motivation. Our previous work will be shown to give us a good understanding of the torsion points of elliptic curves in global fields. This will be an excellent source of computational examples to work with. We will also deduce the Lutz-Nagell theorem and give a consequence toward the congruent number problem.

Potential Talks: Computational examples

Elliptic Curves over Global Fields: Mordell-Weil Theorem We will work intently toward the Mordell-Weil theorem, which states that the abelian group of points of an elliptic curve over a number field is finitely generated. This involves first giving some number-theoretic background on class groups and Galois cohomology, e.g. Kummer theory. We can then prove the "weak" Mordell-Weil theorem, and after defining a notion of height on an elliptic curve, prove the Mordell-Weil theorem.

Potential talks: Algebraic number theory background review (class groups, Kummer theory)

Calculations of Rank: We will introduce the notions of Selmer group and Tate-Shafarevich group, and outline their influence on rational points of elliptic curves, particularly the rank. In general the rank is hard to predict, but we will describe some situations where it can be calculated by performing a "descent."

Potential talks: Review of Galois cohomology

The following topics may round out the latter parts of the course. Probably not all of these will be able to be discussed, but some parts of them will be selected based on student preference.

Modularity of Elliptic Curves: The modularity of elliptic curves was proven through the 1990s, with consequences such as Fermat's last theorem. In this potential topic, we will introduce modular curves and modular forms up to the level to understand what it means for an elliptic curve to be modular. Computational examples can illustrate this explicitly.

Potential talks: Modular curves over $\mathbb{C}$ and modular forms; the Jacobian variety of an algebraic curve

The Birch and Swinnerton-Dyer conjecture: The content of the course up to this point needs only a bit more augmentation in order to state the Birch and Swinnerton-Dyer conjecture. In this potential topic, we will cover this gap by introducing the period, regulator, and L-function of an elliptic curve over a number field, and then give a discussion of the content of the conjecture.