MATH 682 R1 *Introduction to Elliptic Curves*

Lectures: January 7 - April 11
MWF 12:00 - 12:50 CAB 457
No classes on February 18-22, Friday March 21, Monday March 24

Instructor: Matilde N. Lalín
CAB 621, office hours Mondays 1:00 - 2:00, Wednesdays 10:00 - 12:00, and by appointment
`lalin@ualberta.ca`
`www.math.ualberta.ca/~mlalin/math682`

Textbook: J. S. Milne , *Elliptic Curves*, BookSurge Publishers 2006.
Available for purchase at `www.jmilne.org/math/Books/index.html`,
and for free at `www.jmilne.org/math/Books/ectext.html`
Other books: J. Silverman, The Arithmetic of Elliptic Curves;
N. Koblitz, Introduction to Elliptic Cuves and Modular Forms; A. Knapp, Elliptic Curves; J. Cassels, Lectures on Elliptic Curves; J. Silverman and J. Tate, Rational Points on Elliptic Curves.

Assignments: They will be posted on the website. They will be due in class as follows: January 23, February 6, February 27, March 12, March 26, April 9.
Late assignments will not be accepted.

Weights: The midterm and each of the homework assignments will have the same weight. The worst of the seven marks will be dropped. There will be no final exam.

Exam Dates: Midterm Exam - Friday March 28, 2008, in class.

Grading: Based on a combination of absolute measures and distribution.

General Description: One of the big problems in number theory concerns the resolution of polynomial equations in integers or rational numbers (Diophantine equations). Polynomials of degree 1 or 2 are well-understood. Now, the next natural step is to look at equations of degree 3. Essentially an elliptic curve is defined by an equation

$$y^2 = x^3 + ax + b.$$

It turns out that the rational solutions to this equation form a group, which is abelian and finitely generated (Mordell's theorem). Understanding the rank of this group involves a famous conjecure (Birch–Swinnerton-Dyer) which resolution is worth a million dollars.

Elliptic curves show up in many areas (that look unrelated), such as congruent numbers, sphere packing, factorization of integers, etc. They are also related to modular forms which is the starting point for the proof of Fermat's Last Theorem.

Syllabus: The goal of this class is to study as much as possible about the basics of elliptic curves. We plan to chapters 1-4 of Milne's book, and cover chapter 5 as time permits. Tentatively:

1. Plane curves, Cubics, group structure in cubics.
2. Definition of elliptic curves, Weierstrass equation, elliptic curves modulo p, torsion points
3. Complex structure of elliptic curves.
4. Arithmetic of elliptic curves. Groups of Selmer and Tate-Shafarevich, Mordell theorem, elliptic curves over finite fields, Birch–Swinnerton-Dyer conjecture.
5. Elliptic Curves and modular forms. Modular forms, L-series of elliptic curves, Fermat.

Academic Integrity: The University of Alberta is committed to the highest standards of academic integrity and honesty. Students are expected to be familiar with these standards regarding academic honesty and to uphold the policies of the University in this respect. Students are particularly urged to familiarize themselves with the provisions of the Code of Student Behaviour (online at `www.ualberta.ca/secretariat/appeals.htm`) and avoid any behaviour which could potentially result in suspicions of cheating, plagiarism, misrepresentation of facts and/or participation in an offence. Academic dishonesty is a serious offence and can result in suspension or expulsion from the University.

Policy about course outlines can be found in section 23.4(2) of the University Calendar.

Students with Disabilities: Students who require accommodation in this course due to a disability are advised to discuss their needs with Specialized Support & Disability Services (2-800 Students Union Building).

Disclaimer: Any typographical errors in this Course Outline are subject to change and will be announced in class.