MATH 682 R1 *Introduction to Elliptic Curves*

Instructor: Matilde N. Lalín, CAB 621, mlalin@math.ualberta.ca

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 (the reason for that can be found in geometry!). 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 ☺.

I have a truly marvelous outline for this class which this page is too small to contain

Book: I will follow the structure of J. Milne, Elliptic Curves, while freely borrowing material from the 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.

Syllabus: Here is the index of Milne's book, which works well as a tentative, admitedly possibly unrealistic syllabus

1. **Plane Curves**. Definitions, Bezout's theorem, Rational points on plane curves, Group law on a cubic curve, Regular Functions, Riemann–Roch theorem, Algebraic Curves over subfields.

2. **Basic Theory of Elliptic Curves**. Definition, Weierstrass equation, Reduction modulo p, Elliptic curves over $\mathbb{Q}_p$, Torsion points, Néron models.

3. **Elliptic Curves over the Complex Numbers**. Lattices and bases, Doubly periodic functions, Elliptic curves as Riemann surfaces.

4. **The Arithmetic of Elliptic Curves**. Group cohomology, Selmer and Tate–Shafarevich groups, the finiteness of the Selmer group, Heights, Mordell theorem, rank of $E(\mathbb{Q})$, Néron–Tate pairing, Failure of the Hasse (local-global) principle, Elliptic curves over finite fields, Birch–Swinnerton-Dyer conjecture, Elliptic curves and sphere packings.

5. **Elliptic Curves and modular forms**. The Riemann surfaces $X_0(N)$, $X_0(N)$ as an algebraic curve over $\mathbb{Q}$, Modular forms, L-series of elliptic curves, How to get an elliptic curve from a cusp form, Why the L-series of E_f agrees with the L-series of f, Wiles's proof, Fermat, at last.

*Certain restrictions on the characteristic apply