MATH 381 – Topics in Algebra: An Introduction to Elliptic Curves

Description: This course will cover elliptic curves over the real numbers, the rational numbers, finite fields, and to a limited extent, the complex numbers. The focus of the course will be on the existence of rational points on elliptic curves and the structure of the set of rational points. The application of elliptic curves to the problem of factoring large integers will be presented as well as the role of elliptic curves in the proof of Fermat's Last Theorem.

Prerequisites: Math 330 or permission of instructor.

Text: *Rational Points on Elliptic Curves*, by J. Silverman and J. Tate, Springer-Verlag

Evaluation: The evaluation for the course will be based on problem sets, short writing assignments, a project involving either Maple or Mathematica, a mid-term, and a final exam.

Content Outline:

1. Introduction to Elliptic Curves through Conic Sections (Rational Points and Group Structure)
2. Definition of an Elliptic Curve
3. Group Structure on an Elliptic Curve
4. Normal Forms of Equations
5. Points of Finite Order
6. The Discriminant
7. Complex Analysis (Introduction)
8. Nagell-Lutz Theorem
9. Mordell's Theorem
10. Curves over Finite Fields
11. Integer Points on Elliptic Curves
12. Factorization Algorithm using Elliptic Curves
13. Elliptic Curves in Projective Space
14. The Role of Elliptic Curves in the proof of Fermat's Last Theorem

Learning Outcomes: Upon successful completion of this course, a student will:

- Be conversant with the specialized vocabulary of the topic,
- Be adept with manipulation of the standard notation of the topic,
- Be able to solve routine problems specific to the topic,
- Be able to quote the important assumptions and results (main theorems) of the topic,
- Be able to rigorously prove results specific to the topic, and
- Appreciate the relationship of this topic to the undergraduate mathematics program.