Topics in Number Theory: Elliptic Curves
Math 997 – Spring 2008

Professor: Jennifer Paulhus (paulhus@math.ksu.edu - CW 125)

Prerequisites: Math 730 or equivalent

Textbook: Silverman, Joseph. *The Arithmetic of Elliptic Curves.* Springer Graduate Texts in Mathematics, vol. 106.

Elliptic curves have had a profound influence on a range of modern number theory areas. A crucial part of the proof of Fermat's Last Theorem involves showing that there is no elliptic curve with a certain property. Elliptic curves in cryptography have been heavily studied and utilized in recent years. They are a good starting point for understanding abelian varieties (varieties with a group structure associated to them).

The study of elliptic curves provides a convergence of algebra, number theory, and geometry. In particular, points on elliptic curves have a natural group structure which we will study.

We will talk about elliptic curves over finite fields where we can ask questions about counting all the points and where there are applications to cryptography. We will talk about elliptic curves over $\mathbb{C}$ where the curves may be thought of as isomorphic to $\mathbb{C}$ modulo a lattice (as Riemann surfaces). And we will talk about elliptic curves over global fields where we will prove the Mordell-Weil Theorem which says that, over certain fields, the points on an elliptic curve are a finitely generated group. The study of this group for different curves has motivated much research in the field over the last 20 years.

If time permits, we will discuss some open questions on elliptic curves and related topics. No previous knowledge of curves or varieties will be assumed.

For more information about the course, please contact Jennifer Paulhus.