Course Offering for Spring 2012:
Math 5114 (Specialized Topics in Algebra): Elliptic Curves

CRN 14414
Meets 9:05—9:55 a.m. MWF in McBryde 240
Instructor: Ezra Brown (ezbrown@math.vt.edu)
Prereq: Math 4124 (Abstract Algebra) or its equivalent.

Elliptic Curves are among the most beautiful and elegant and useful of mathematical objects. We find them at the intersection of algebra, algebraic geometry, complex analysis, cryptography, modular forms, number theory, projective geometry, and special functions. An elliptic curve is an abelian group, a torus, a one-dimensional variety, a projective curve, a Diophantine equation, and a modular form. Elliptic curves first appeared seventeen centuries ago in Diophantus’ Arithmetica and attracted the attention of such mathematical luminaries as Fermat, Newton, Euler, Abel, Jacobi, Weierstrass, and Poincare. The last half of the twentieth century found elliptic curves as the objects of intense investigation, and the last thirty years have shown how useful they are. Their fundamental role in the proof of Fermat’s Last Theorem and their essential place in public key cryptography are two examples of their usefulness. One of the Clay Mathematics Institute’s seven millennial problems is the Birch—Swinnerton-Dyer Conjecture, which deals with the rank of the group of rational points on elliptic curves.

In this course, we will study the basic theory of elliptic curves; elliptic curve cryptography; and elliptic curves over the rational numbers, the complex numbers, and finite fields. For further information, please email me at ezbrown@math.vt.edu.

Math 5114 is a topics course, and so it may be taken again for credit provided the contents of the classes taken are different. (The last time Math 5114 was taught as a course in Elliptic Curves was Spring 2005.)