Mathematics 574 Topics in Number Theory Fall 2004

MW 2:50–4:10 Hill 425 J. Tunnell

An elliptic curve over a field K is an algebraic curve defined by an equation of the form $y^2 = x^3 + Ax + B$ $(A, B \in K)$ where the cubic on the right has distinct roots. Of paramount importance in the theory is that the set of solutions (x, y) to these equations with coordinates in a field L containing K form a group (three points on the intersction of a line with the graph of the curve sum to 0 in this group). We will study this group for K the complex numbers, finite fields and number fields. The group structure on the set of points on a elliptic curve allows an array of technical tools such as ℓ–adic representations, Galois cohomology, group schemes, and Selmer groups to be utilized to analyze problems.

The abstract tools used to study elliptic curves must ultimately be brought to bear on specific number theoretic problems. Which integers are the areas of right triangles with integer sides? When is an integer the sum of two rational cubes? Each of these questions leads to open problems in rational points on elliptic curves. We will emphasize examples as a means of exploring the many open problems and conjectures. Much of the theory will be illustrated by special curves such as $y^2 = x^3 - Dx$ or $y^2 = x^3 + D$ which are related to the classical problems above. These elliptic curves exhibit many of the phenomena present in general elliptic curves which arise in many areas of mathematics.

Topics will include the following :

1. The group law for adding points on an elliptic curve
2. Elliptic curves over complex, real, finite and p-adic fields
3. The group of rational solutions to $E : y^2 = x^3 + Ax + B$ form a finitely generated abelian group (the Mordell-Weil group of E)
4. Effective bounds on the rank of the Mordell-Weil group
5. Conjectural effective algorithms to find all rational solutions to $y^2 = x^3 + Ax + B$
6. L-series of elliptic curves and relations to modular curves
7. Applications to classical Diophantine problems

Prerequisites: We will assume no prior knowledge of elliptic curves and will assume no more than an introductory graduate number theory course.

Text: The text for this course will be **Arithmetic of Elliptic Curves** by J.H. Silverman. This text is a standard reference in the field. Other texts will be on reserve and notes will be distributed for certain topics.

Course Format: There will be periodic problem assignments and term projects involving elliptic curves.

More Information: Contact J. Tunnell in Hill 546, email to `tunnell@math` or consult `http://www.math.rutgers.edu/~tunnell/math574.html`