Math 207C

Elliptic Curves

Elliptic curves lie at the heart of contemporary number theory, and a basic understanding of them is key to graduate work in the field. They also arise naturally in a number of other fields including cryptography and combinatorics. This introductory course will define them in a general setting and prove the basic results. Examples include the Mordell-Weil theorem and the computation of the Mordell-Weil group, the Riemann Hypothesis for elliptic curves over finite fields, and the Schoof-Elkies algorithm for computing the group of points, the theory of the non-abelian Galois extensions generated by torsion points, the theory of the height pairing (and applications to sphere packing), and the theory of supersingular curves and recent applications to construction of expander graphs and hash functions in cryptography, the Tate-Shafarevitch group, the theory of reduction mod p, the connection(s) with modular forms, the Shimura-Taniyama Conjecture (now a theorem of Wiles and others) and the Conjecture of Birch and Swinnerton-Dyer.

The course will require no background other than a mastery of the basic grad algebra syllabus and some complex analysis. A parallel introduction to algebraic geometry, taught by Hida this quarter, will give needed background from that area. However, results from that field (such as the Riemann-Roch theorem) will be carefully stated, if not proven in this course.

The course meets Monday and Wednesday, 3-4:15 in MS 7608.

There will be homework assignments and a final study project, with classroom presentation, for evaluation. The subject is sufficiently rich that all students (even those primarily interesting in analysis) should be able to find a topic that interests them.

For further information, please email me. The first lecture will state some of the target theorems and begin the theory of elliptic functions, i.e. we will start the course over C, with doubly periodic meromorphic functions in the the complex plane.

Don Blasius