An introduction to the arithmetic of elliptic curves

Kirti Joshi

Elliptic curves have a ubiquitous role in mathematics and in number theory. These curves play a central role in many diverse situations -- mathematical physics, cryptography, Wiles' proof of Fermat's last theorem, and many more. Here is a problem of classical geometry (considered by ancient greek mathematicians): given a rational nunber n, find a right angled triangle with area n and with rational sides. Finding such a right angled triangle is equivalent to finding rational solutions of the equation

$$y^2 = x^3 - n^2 x.$$

This happens to be an elliptic curve! This curve may or may not (depending on n) have rational solutions other than the ``trivial'' ones corresponding to x=0, +n, -n, y=0.

With this introduction let me say more about the course. This is a standard course on the arithmetic of elliptic curves. We will begin with basic definitions and go on to cover the group law on elliptic curves, the proof of the Mordell-Weil Theorem (which describes the structure of this group law for rational solutions), elliptic curves over finite fields (this will be useful for anyone who want to uderstand applications of elliptic curves to cryptography--though we will not be interested in cryptography for this course), reduction modulo p of elliptic curves, the semi-stable reduction theorem, computations of the Mordell-Weil group and finally we will discuss L-functions of elliptic curves and the Birch-Swinnerton-Dyer conjecture.

I will keep the course self contained-but it will be a good idea to also sign up for the algebraic geometry course being offered in fall. Elliptic curves are algebraic curves and as such prove a valuable testing ground for algebraic geometry of curves (beyond the easy case of conics and lines) and this two course combination will be useful for students who wish to pursue/explore algebraic geometry/number theory for their research. Nevertheless I would like to emphasize that this course will be self contained. As for the course requirements: the core algebra course should suffice, but if you have taken the number theory course then that would be perfect.

If you have any questions or if you are interested in taking this course, do let me know.