

(3-0-0; —)

Introduction to Elliptic Curves

MATH-495*

This will be an introduction to the arithmetic theory of elliptic curves. We will begin with the celebrated theorem of Mordell and Weil on the finite generation of rational points on a given elliptic curve over the rational number field. Then, we will discuss the structure of the torsion subgroup as embodied by the Lutz-Nagell theorem. Afterwards, we discuss elliptic curves over finite fields and prove the “Riemann hypothesis” for zeta functions of elliptic curves over a finite field. The course will conclude with a discussion of the “million-dollar” problem of the Birch and Swinnerton-Dyer conjecture.

Textbook: *Rational Points on Elliptic Curves*
by J. Silverman and J. Tate (Springer-Verlag)

Prerequisite: MATH-313* and MATH-314*.

Instructor: Ram Murty

Evaluation: Homework (five assignments) 100%

Outline:

1. Mordell-Weil Theorem
2. Lutz-Nagell Theorem
3. Heights on elliptic Curves
4. Elliptic Curves over Complex Numbers
5. Elliptic Curves over Finite Fields
6. Exponential Sums and Zeta Functions of Elliptic Curves