CS 6101 : MATHEMATICAL FOUNDATIONS OF COMPUTER SCIENCE

Monsoon 2015. Lecture Room: ELHC 203.
Timings: Tue 11:15-12:15, Wed: 8:00-9:00, Fri: 9:00-10:
Instructor: K. Murali Krishnan.

Course Objectives:

The course aims at a graduate level treatment of a certain algebraic, combinatorial and probabilistic methods that form the building blocks of algorithms in modern cryptography, coding theory, signal processing, big data analytics etc.

Course Outcomes:

At the end of the course, the student is expected to attain an adequate level of proficiancy in some of mathematical methods necessary to understand the literature in the fields mentioned above. The training given in the course is expected to make the student mathematically mature enough to be able to self study topics in mathematics that may be necessary for pusuing her/his area of research in computer science.

Methodology:

The lectures will focus on concrete algorithms like the Miller-Rabin primality test, the Fast Fourier Transform algorithm, the Lagrange-Gauss algorithm for lattice basis reduction and the Karger's Max-Cut algorithm, Factorization of polynomials over finite fields etc., completly covering the necessary mathematical pre-requisites. Part of the material will be developed through assignments, which the students are expected to work out. Assignment problems and supplimentary reading material will be posted on the course web page
http://athena.nitc.ac.in/~kmurali/Courses/MFCS15/index.html.

Summary of Contents Covered:

Algebraic Methods: Structure theory of cyclic groups, Gauss theorem of cyclicity of prime fields, Fermat's test, Carmichael numbers, Miller Rabin test, Quadratic reciprocity, Solovey Strassen primality test.
Integer lattices in the plane, Gauss-Lagrange basis reduction algorithm. Structure of finite fields, Berlekamp's polynomial factorization algorithm, Cooley and Turkey Fast Fourier Transform Algorithm.

Combinatorial and Probabilistic Methods: Tail bounds for discrete random variables, Chernoff bound, Randomized graph Max Cut algorithms, De-randomization using conditional expectation.

Evaluation:

There will be three examinations, the first two carrying 30% weightage and the final carrying 40% weightage. The students are expected to have solved assignment problems before appearing for the tests. Marks earned in additional tests (if any) will be adjusted against the credits of the three main examinations.