CS 4031 : Computational Algebra

Winter 2016. Lecture Room: ELHC 402.
Timings: Mon 11:15-12:15, Tue: 8:00-9:00, Thu: 9:00-10:
Instructor: K. Murali Krishnan.

Course Objective:

An advanced undergraduate treatment of algorithms and design techniques in the field of algorithmic number theory and algebra.

Course Outcomes:

At the end of the course, the student is expected to attain proficiancy in the mathematical techniques like Chinese remaindering, Hensel lifting and the Fourier Transform method. The student will also be able to analyse basic algorithms for lattice basis reduction, primality testing, polynomial factorization over finite fields and describe how these algorithms find application to public key encryption, decoding Reed Solomon codes etc.

Methodology:

The lectures will focus on concrete algorithms like the Solvey Strassen and Aggarwal-Kayal-Saxena algorithms for primality testing, the Fast Fourier Transform algorithm and its application to polynomial multiplication, the Lagrange-Gauss algorithm for lattice basis reduction and the Berlikamp and Cantor-Zassenhaus algorithms Factorization of polynomials over finite fields. The necessary mathematical pre-requisites will be completely coverexd in the course. 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/17CompAlgebra/index.html.

Summary of Contents Covered:

Review of basic number theory and algebra, Fermat's test, Carmichael numbers, Miller Rabin test, Quadratic reciprocity, Solovey Strassen primality test, Aggarwal Biswas algorithm and the Aggarwal Kayal Saxena Algorithm. Hensel lifting and polynomial division, Integer lattices in the plane, Gauss-Lagrange basis reduction algorithm. Structure of finite fields, Berlekamp's polynomial factorization algorithm, Cantor-Zassenhaus factorization algorithm, Cooley-Turkey FFTransform Algorithm, Polynomial interpolation, Berlikamp-Welsh decoding algorithm for Reed Solomon codes, Sudan-Guruswamy list decoding algorithm for Reed Solomon codes.

Evaluation:

There will be two or more internal examinations, carrying a total 60% weightage and a final exam carrying 40% weightage. The students are expected to have solved the assignment problems before appearing for the tests.