COMPUTATIONAL NUMBER THEORY AND ALGEBRA

PROF. NITIN SAXENA
Department of Computer Science and Engineering
IIT Kanpur

PRE-REQUISITES : Preferable (but not necessary)-- Theory of Computation, Algorithms, Algebra

INTENDED AUDIENCE : Computer Science & Engineering, Mathematics, Electronics, Physics, & similar disciplines.

INDUSTRY SUPPORT : Cryptography, Coding theory, Computer Algebra, Symbolic Computing Software, Cyber Security, Learning Software

COURSE OUTLINE :

Algebra plays an important role in both finding algorithms, and understanding the limitations of computation. This course will focus on some of the fundamental algebraic concepts that arise in computation, and the algebraic algorithms that have applications in real life. The course will cover the problems of fast integer (or polynomial) multiplication (or factoring), fast matrix multiplication, primality testing, computing discrete logarithm, error-correcting codes, lattice- based cryptography, etc. The course intends to introduce both basic concepts and practical applications.

ABOUT INSTRUCTOR :

Prof. Nitin Saxena has completed my Bachelors in Computer Science from the Indian Institute of Technology, Kanpur in 2002 and completed my PhD under Manindra Agrawal in 2006. He is broadly interested in Computational Complexity Theory, Algebra, Geometry and Number Theory. He has been a visiting graduate student in Princeton University (2003-2004) and National University of Singapore (2004-2005); a postdoc at CWI, Amsterdam (2006-2008) and a Bonn Junior Fellow (W2 Professor) at Hausdorff Center for Mathematics, Bonn (2008-2013). Since April 2013, He has a faculty position in the department of CSE, IIT Kanpur.

COURSE PLAN :

Week 1: Outline. Notation. Background.

Week 2:GCD. Chinese remaindering. Fast polynomial multiplication.

Week 3: Fast integer multiplication. Fast integer division. Fast gcd.

Week 4: Fast matrix multiplication. Tensor rank.

Week 5: Factorization over finite fields.

Week 6: Berlekamp, Cantor-Zassenhaus factoring algorithms.

Week 7: Reed-Solomon code. List decoding. Bivariate polynomial factoring.

Week 8: Kaltofen's blackbox multivariate factoring.

Week 9: Integral polynomial factoring. LLL algo. Shortest vector in lattice.

Week 10: Lattice-based cryptography.

Week 11: Primality testing. RSA cryptosystem. Diffie-Hellman. Discrete Log.

Week 12: Integer factoring. Pollard, Fermat, Morrison-Brillhart, Quadratic sieve methods.