Course announcement

Algebra and Computation (MIT 6.S897)

Prereq: 6.840 + 6.046 + 18.703
Time: MW 11:00-12:30pm
Location: 34-304
3-0-9 H-Level Grad Credit
Homepage: http://people.csail.mit.edu/madhu/ST15/

Ever wondered why we can find the greatest common divisors of two integers, without knowing how to factor either? Why are polynomials easy to factor when integer factorization seems hard? Algorithms associated with algebraic operations are often extremely surprising. They are also quite ingenious - who would have thought that the identity "x^q - x = prod_{a in F_q} (x-a)" can be an algorithmic tool? Why is randomness such a powerful tool in algebraic algorithms often giving exponential speedups on best known deterministic algorithms? And what do algebraic algorithms have to do with the Rubik's cube? In this course we will explore some of these questions and use them as a motivation to study algebra and computing a bit more systematically.

- The first part will cover some strikingly efficient algorithms in Algebra, Number Theory, and Group Theory. Some topics include algorithms for membership testing in groups, factoring polynomials (Berlekamp, Lenstra-Lenstra-Lovasz, Kaltofen etc.), algorithms for testing primes (Agarwal-Kayal-Saxena), solving systems of polynomial equations, ideal membership.
- The second part of the course will focus on the interplay between complexity theory and algebra as highlighted by algebraic versions of the P vs. NP question. Introduction to the Valiant and Blum-Shub-Smale models of arithmetic complexity.Role of the permanent and determinant. Depth-reduction in arithmetic complexity. Connection between deterministic polynomial identity testing and lower bounds for the permanent.

See http://people.csail.mit.edu/madhu/FT98, http://people.csail.mit.edu/madhu/FT05 and http://people.csail.mit.edu/madhu/ST12 for details of earlier versions of this course.

Instructor: Madhu Sudan

Alert: Please email Madhu asap if you are interested in the course.