

POMONA COLLEGE

COMPUTER SCIENCE COLLOQUIUM

Fast Algorithms on Polynomials

Chris Umans

Caltech

Abstract: Factoring integers is believed to be computationally hard, so it's perhaps surprising that *polynomials* can be factored in polynomial time. The key to the fastest known algorithms for polynomial factorization is modular composition (the problem of composing two polynomials modulo a third). I'll describe some of the ideas that go into a new, faster algorithm for modular composition -- the first progress on this problem in quite some time. This leads to faster polynomial factorization algorithms, which in turn have applications to decoding error-correcting codes.

The talk will be self-contained -- I'll review just a couple of basic algebraic concepts that are necessary to describe some of the ideas.

Thursday, February 7 at 4:15 pm

Rose Hills Theater – Smith Campus Center

Pomona College

Refreshments available at 4:00