Complexity upper bound for a sieving algorithm

Robin Pemantle
University of Pennsylvania

Thursday, September 30, 2010
007 Kemeny Hall, 4:00 pm
(Tea 3:30 pm 300 Kemeny Hall)

Abstract

Central to many factoring algorithms in use today is the following random process: generate random numbers in the interval [1,N] until some subset has a product which is a square. Naive probabilistic models for the distribution of prime factors suggest that this stopping time has a sharp threshold. Based on more sophisticated probabilistic models, we find a rigorous upper bound that is within a factor of 4/pi of a proven lower bound, and conjecture that our upper bound is in fact asymptotically sharp. This is joint work with Andrew Granville, Ernie Croot and Prasad Tetali.

This talk should be accessible to graduate students.