STANFORD PROBABILITY SEMINAR

Prasad Tetali, Georgia Tech
Monday, 15 May 2006
4:15pm (Refreshments at 4pm in the 1st Floor Lounge)

ROOM CHANGE: The talk will be in 380-380C

On the Sharp Threshold for the Square Dependence Problem

Abstract. Motivated by a common subproblem occurring in several factoring algorithms, in 1994 C. Pomerance introduced the so-called square dependence problem: select integers sequentially at random from the interval $[1, x]$, for some large $x$, and stop once the product of a subsequence of the chosen integers is a square; the problem is to determine (as a function of $x$) the stopping time of this process. Pomerance and Schroeppel estimated the stopping time to lie in an interval $[y, y^{1+o(1)}]$, for an appropriate $y = y(x)$. We tighten this interval significantly to $[y, cy]$, for a small positive constant $c$. This is joint work with Andrew Granville and Ernie Croot.