

STATISTICS COLLOQUIUM

THURSDAY, NOVEMBER 13, 2008

Talk: 4:30 PM – *Science Center 309*

Reception: 5:45 PM – *Science Center, 7th Floor*

“An Upper Bound on the Time for Quadratic Sieving”

Robin Pemantle

University of Pennsylvania

Department of Mathematics

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 (and there is a computable witness to this).

Naive probabilistic models for the distribution of prime factors suggest that this stopping time has a very sharp threshold. Based on more sophisticated probabilistic models, we find a rigorous upper bound that is within a factor of $4/3$ 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.