

ATELIER «NOUVELLES AVENUES EN PROCESSUS SPATIAUX ALÉATOIRES»  
11–15 MAI 2009

WORKSHOP “NEW DIRECTIONS IN RANDOM SPATIAL PROCESSES”  
MAY 11–15, 2009

How many random integers from 1 to  $N$  must you see before some subset has a  
square product ?

ROBIN PEMANTLE

Department of Mathematics  
University of Pennsylvania  
David Rittenhouse Lab., 209 S. 33rd Street  
Philadelphia, PA 19104-6395  
USA

pemantle@math.upenn.edu

---

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  $\frac{4}{3}$  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.*