1031-11-86 **Prasad Tetali*** (tetali@math.gatech.edu), 686 Cherry Street, Georgia Tech, Atlanta, GA 30332-0160. *Collision Time in Pollard's Rho for the Discrete Log Problem.*

We analyze a standard version of Pollard's Rho algorithm for finding the discrete logarithm in a cyclic group G. Affirming a widely believed conjecture, we prove that, a collision occurs in $O(\sqrt{|G|})$ steps, with high probability. Our proof is based on a second moment argument and on analyzing (using Fourier techniques) an appropriate nonreversible, non-lazy random walk on a discrete cycle of (odd) length. This is joint work with Jeong Han Kim, Ravi Montenegro, and Yuval Peres. (Received August 04, 2007)