Lucas Dachman
CSCI 2824
HW8

Homework 8: Prime Factorization

This program uses Pollard's Rho Algorithm to find prime factors p and q such that p*q=N where N is composite. Pollard's Rho Algorithm uses the fact that the probability of picking two equal random numbers from a list of t random numbers from 1 to N is 50% if $t > 1.177N^{1/2}$. Similarly, we will have the same probability of finding two numbers who's difference is a factor of N. More generally, $GCD(x_1 - x_2, N) = p$. The algorithm uses a pseudo random sequence, f(x) = x*x + seed mod N where the seed changes when a cycle has been detected. The program uses Floyd's cycle-finding algorithm to detect repetition. On each loop, a is set to f(a) and b is set to f(f(a). when f(a) = f(f(a), a cycle has been detected and the seed in f(x) is changed.

How To Run

First compile with 'make'. Then run './fact <number>'. Running './fact' with no arguments outputs a usage message.