

# Computer Science 2300: Homework 1

Due: January 29, 2008

**Note:** Please use rigorous, formal arguments. You will not receive full credit otherwise.

1. (10 points, Based on a question from Cormen *et al*'s *Introduction to Algorithms*) Consider the following procedure for generating a permutation of the numbers  $1 \dots n$ . First, choose an integer  $r$  uniformly at random between 1 and  $n$ . Now consider the array  $A$  with indices from 0 to  $n - 1$ . Fill  $A[i]$  with the number  $i + r + 1$  if  $i + r + 1 \leq n$  and with the number  $i + r + 1 - n$  otherwise. First show that each number between 1 and  $n$  has a  $1/n$  probability of winding up in any particular position in  $A$ . Then show that the resulting permutation in  $A$  is not uniformly random.
2. (10 points) Problem 0.3 (page 9) in the DPV text
3. (10 points) Let  $A, B, N, P$  be positive integers with  $A > B$  and  $A \equiv B \pmod{P}$ . Prove that  $A^N \equiv B^N \pmod{P}$ .
4. (10 points) Problem 1.15 (page 39) in the DPV text
5. (10 points) Problem 2.3 (page 71) in the DPV text
6. (10 points) Problem 2.4 (page 71) in the DPV text