COL202: Discrete Mathematical Structures
Tutorial/Homework: 07

1. Discuss Quiz-05 in case required.
2. Consider the following algorithm that takes as input an integer array A and its size n.

```
FunnyAlgo(A, n)
  - if (n < 2^20)
     - for i = 1 to n − 1
         - for j = 1 to i
             - A[j + 1] ← A[j] + 1
  - else
     - for i = 2 to n
         - A[i] ← A[i] + A[i − 1]
```

   (a) State true or false: The running time is $O(n^2)$?
   (b) State true or false: The running time is $\Omega(n)$?
   (c) State true or false: The running time is $\Omega(n^2)$?
   (d) Write the running time of the algorithm in Θ notation. That is give a tight bound on the worst-case running time of the above algorithm.

3. Consider the following problem:

   SAME-OUTPUT: Given descriptions $\langle A \rangle, \langle B \rangle$ of decision algorithms A and B respectively, determine if both algorithms halt with the same output on all inputs.

   A decision algorithm is one that either outputs 0 (exclusive-or) 1. An algorithm P is said to solve the above problem if $P(\langle A \rangle, \langle B \rangle)$ halts and outputs 1 when A and B halt on all inputs with the same output, and it halts and outputs 0 otherwise. Does there exist an algorithm P that solves the problem SAME-OUTPUT?

4. Find counterexamples to each of these statements about congruences:

   (a) If $ac \equiv bc \ (mod\ m)$, where a, b, c, and m are integers with $m \geq 2$, then $a \equiv b \ (mod\ m)$.

(b) If $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, where a, b, c, d, and m are integers with c and d positive and $m \geq 2$, then $a^c \equiv b^d \ (mod\ m)$.

5. Show that if a and b are both positive integers, then $(2^a - 1) \ (mod\ (2^b - 1)) = 2^{a \ (mod\ b)} - 1$.

6. (a) Show that the positive integers less than 11, except 1 and 10, can be split into pairs of integers such that each pair consists of integers that are inverses of each other modulo 11.

   (b) Use part (a) to show that $10! \equiv -1 \ (mod\ 11)$.

7. Prove that an integer $(a_{n-1}, ..., a_0)$ is divisible by 11 if and only if $a_0 + a_2 + a_4 + ... \equiv a_1 + a_3 + ... \ (mod\ 11)$.