**COL202: Discrete Mathematical Structures**
**Tutorial/Homework:** 08

1. Discuss Quiz-06 (in case required).

2. Design an algorithm that takes as input positive integers $a, b, m$ and outputs $a^b \ (mod\ m)$ (input/output is in binary). Discuss the worst-case time complexity of your algorithm.

3. Recall the Euclid-GCD$(a, b)$ algorithm discussed in the lectures for finding the gcd of two integers $a$ and $b$. Prove the following theorem:

   **Theorem 8.0.1 (Lame's theorem)** *For any integer $k \geq 1$, if $a > b \geq 1$ and $b < F_{k+1}$, then the call Euclid-GCD$(a, b)$ makes fewer than $k$ recursive calls.*

   Here $F_k$ denotes the $k^{th}$ number in the Fibonacci sequence $(0, 1, 1, 2, 3, 5, 8, 13, ...)$

4. You must have seen the following puzzle: You are given two jugs, one of capacity 5 litres and another of capacity 3 litres, and there is an unlimited source of water. Using just these two jugs, can you make sure that the larger jug has exactly 4 litres of water?

   (a) Solve the above puzzle.

   (b) Now suppose you are given two jugs with capacities $S, L$ that are positive integers. Design an algorithm that takes as input a positive integer $B$ and outputs "Not Possible" if it is not possible to leave $B$ litres of water in any of the two jugs and otherwise it outputs the precise way to make sure that one of the jugs has exactly $B$ litres of water.

5. Discuss the closure property of multiplication modulo $m$ with respect to $\mathbb{Z}_m^\star$.

6. Show that if $p$ is prime, the only solutions of $x^2 \equiv 1 \ (mod\ p)$ are integers $x$ such that $x \equiv 1 \ (mod\ p)$ or $x \equiv -1 \ (mod\ p)$.