COL202: Discrete Mathematical Structures
Tutorial/Homework: 09

1. Discuss Quiz-07 (in case required).

2. Problems from the lecture:

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

   (b) Complete the three exercises on group theory mentioned in the class (Slide 3 of 20th September).

   (c) Prove the theorem of group theory (Slide 4 of 20th September).

3. (a) Generalize the result in part (a) of problem 6 of Tutorial-07; that is, show that if p is a prime, the positive integers less than p, except 1 and $p-1$, can be split into $(p-3)/2$ pairs of integers such that each pair consists of integers that are inverses of each other.

   (b) From part (a) conclude that $(p-1)! \equiv -1 \ (mod\ p)$ whenever p is prime. This result is known as *Wilson's theorem*.

   (c) What can we conclude if n is a positive integer such that $(n-1)! \not\equiv -1 \ (mod\ n)$?

4. Let $N = p \cdot q$ for primes p and q. Let $e, d \in \mathbb{Z}_{\phi(N)}^*$ such that $e \cdot d \equiv 1 \ (mod\ \phi(N))$, where $\phi(N) = (p-1)\cdot(q-1)$. In the lectures, we have seen that $\forall M \in \mathbb{Z}_N^*, (M^e)^d \equiv M \ (mod\ N)$. Show that this holds for all $M \in \mathbb{Z}_N$.

5. Show that we can easily factor N when we know that N is the product of two primes, p and q, and we know the value of $(p-1)(q-1)$.

6. We will use the following definition of cyclic groups.

   Definition 9.0.1 (Cyclic group) *Let G be a group and let a be any element of this group. Let $\langle a \rangle = \{x \in G | x = a^n \text{ for some } n \in \mathbb{Z}\}$. The group G is called a cyclic group if there exists an element $a \in G$ such that $G = \langle a \rangle$. In this case, a is called the generator of G.*

   Show that for any prime p, Z_p^* is a cyclic group.