CSL202: Discrete Mathematical Structures
Tutorial/Homework: 06

1. 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 16)
   (c) Prove the theorem of group theory (Slide 17).
2. (a) Generalize the result in part (a) of problem 3 of the previous tutorial; 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 $(n-1)! \not\equiv -1 \ (mod\ n)$?
3. 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.
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 1.0.1 (Cyclic group) *Let G be a group and let a be any element of this group. Let $< a > = \{x \in G | x = a^n \text{ for some } n \in \mathbb{Z}\}$. The group G is called a cyclic group if there exists an element $a \in G$ such that $G = < a >$. In this case, a is called the generator of G.*

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

7. Alice wants to communicate a large integer N to Bob over a lossy channel. Over this channel, Alice can send packets of information each containing an integer. However, there is 10% chance that this packet is going to get *dropped* (that is, Bob does not receive the packet) in transit. One solution is to send multiple packets each containing N. The communication overhead (the total number of *digits* communicated across all packets) in this case might be large. Can you think of a way to reduce the communication overhead using the Chinese Remaindering Theorem? Discuss.
(Note that this is a subjective question. For this question, I am only looking for high-level discussion at this time of the course. We might revisit this question at a later stage of the course.)