Assignment 4
CS 203: Discrete Structures

Course Instructor : Prof. Prabuchandran K J

Teaching Assistants : Sagartanu Pal, Tephilla Prince, Ravi Kumar Patel, Sourav Ganguly

INSTRUCTIONS: You have to give clear and detailed solution for each of the questions. **Make one single pdf file containing solutions to all problems. Take a clear picture and upload the hand written solutions in Classroom(event-assignment4) by 8/11/2021, 10 pm. Name your pdf with your** *name_rollno*.**pdf.** For example *harrithha_*200010018.*pdf*. Late submissions will not be graded. Students can discuss but must write their solutions based on their understanding independently. Do not use web resources or answers from your peers to obtain solutions. If anyone is involved in malpractice of any sort, then suitable disciplinary action will be taken. If required, there would be a viva to selected set of students.

1. Determine last 3 digits of 137^{64}. Use the idea of Euler totient function and generalization of Fermat's little theorem taught in the class. You can use Binomial Theorem to verify the answer but can not use it to solve the problem. If you use, no marks will be given. (3)

2. State and prove Chinese Remainder Theorem. Give an example. (3)

3. State and Prove Lagrange's theorem and give an example. (3)

4. Let (A,*) be an Algebraic system such that

$$a * a = a \qquad \forall a \in A$$
$$(a * b) * (c * d) = (a * c) * (b * d) \qquad \forall a, b, c, d \in A$$

   Show that $(a * (b * c)) = (a * b) * (a * c)$. Comment if $(a * (b * c)) = ((a * b) * c)$ (2)

5. Let (A,*) be a monoid such that $x * x = e \;\; \forall x \in A$ where 'e' is the identity element. Show that (A,*) is an Abelian Group. (2)

6. Let G be a group of order p where p is a prime number. What are the subgroups of G? (1)

7. The number of all subgroups of the group $(\mathbb{Z}/60\mathbb{Z}, +)$ of integers modulo 60 is:

   a 2.

   b 12.

   c 60.

   d 10.

   (2)

8. What is the inverse of 37 and 51 in the group $(\mathbb{Z}/87\mathbb{Z})^*$. Clearly describe the steps to compute inverse. (2)

9. Is a group Homomorphism always a group Isomorphism? If not, give a counter example and justify. (2)