CS 203B: Mathematics for Computer Science-III
Assignment 2

Deadline: 18 : 00 hours, August 19, 2015

General Instructions:

- Write your solutions by furnishing all relevant details (you may assume the results already covered in the class).
- You are strongly encouraged to solve the problems by yourself.
- You may discuss but write the solutions on your own. Any copying will get zero in the whole assignment.
- If you need any clarification, please contact any one of the TAs.
- Please submit the assignment at KD-213/RM-504 before the deadline. Delay in submission will cause deduction in marks.

Question 1: [10]

Prove that there is no nontrivial homomorphism from the group $(\mathbb{Q}, +)$ to $(\mathbb{Q}^*, \times)$, where $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. By trivial homomorphism, we mean the homomorphism that maps every element of one group to the identity element of another one.

Question 2: [5+5]

(a) (Euler's theorem) For a number n, say $\phi(n)$ is the number of positive elements co-prime to n and less than n. For any a which is co-prime to n, $a^{\phi(n)} = 1 \pmod{n}$.

Prove this theorem.

(b) Use the group $\mathbb{Z}_p^*$ under multiplication operation to show that if p is a prime number, then $(p-1)! = -1 \pmod{p}$. This theorem is known as Wilson's theorem.

Question 3: [10]

If an abelian group has subgroups of order m and n respectively, then show that it has a subgroup whose order is the least common multiple of m and n.

Question 4: [10]

For any group G, each element $g \in G$ can be identified with a map $G \to G$. Thus, show that every group of order n is isomorphic to some subgroup of S_n.

Question 5: [7+3]

A group G is said to be *cyclic* if there exists an element $g \in G$ such that $G = \{g^i | i \text{ is an integer}\}$ and g is called the *generator* of that cyclic group.

(a) Prove that any subgroup of a cyclic group is itself a cyclic group.

(b) How many generators does a cyclic group of order n have?

Question 6: [10]

Suppose p be an odd prime and if

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{a}{b},$$

where a and b are integers, show that $p|a$.

Question 7: [5+5+10]

There were three errors in the claims made in the class. No one caught it. You need to be more vigilant! In this question, these the errors are fixed.

1. It was claimed that $Z_4 \cong Z_2 \oplus Z_2$. Prove that this is not possible. It was claimed that if $H < G$, G commutative, and $G/H \cong \hat{H} < G$, then $G \cong H \oplus \hat{H}$. This example shows that this is not always true! Think where does the argument shown in the class goes wrong.

2. It was claimed that if G is a finite commuitative group, $|G| = n$, and $n = \prod_{j=1}^{k} p_j^{e_j}$ with p_j's distinct primes, then
$$G \cong Z_{p_1}^{e_1} \oplus Z_{p_2}^{e_2} \oplus \cdots \oplus Z_{p_k}^{e_k}.$$
Give a counterexample to this claim. (Hint: consider $Z_2 \oplus Z_2$.)

   The correct version of the theorem is: if G is a finite commutative group, and $|G| = n$ then
$$G \cong Z_{p_1}^{e_1} \oplus Z_{p_2}^{e_2} \oplus \cdots \oplus Z_{p_k}^{e_k},$$
where p_j's need not be distinct and $n = \prod_{j=1}^{k} p_j^{e_j}$.

3. When are p_j's distinct? Prove that the following statements are equivalent:

   (a) All p_j's are distinct.

   (b) G is a cyclic group.

   (c) The number of solutions in G of the equation $x^m = e$ (e is the identity element) is at most m for every positive integer m.

Question 8: [10]

Let $\phi : G \mapsto G$ be a homomorphism of group G. *Kernel* of ϕ is defined as:

$$K = \{a \in G \mid \phi(a) = e\}.$$

Prove that $K < G$ and $\phi(G) \cong G/K$.