Assignment-3

Submit to Manohar at CSTAR on 11^{th} April, 2014 before 3 p.m.
(Only 11^{th}, no prior/post submissions allowed)

List of notations

1. We say that a *divides* b if b is a integer multiple of a (i.e $b = ka$ for some $k \in \mathbb{Z}$) and it is denoted by $a|b$.

2. For $n \in \mathbb{N}, a \equiv b \mod n$, if $n|(a-b)$.

3. Addition Modulo n ($\oplus_n$): $a \oplus_n b = a + b \mod n$.

4. Multiplication Modulo n ($\otimes_n$): $a \otimes_n b = a \times b \mod n$.

5. For $n \in \mathbb{N}$, $\mathbb{Z}_n = \{1, 2, 3, ..., n\}$.

6. For $n \in \mathbb{N}$, $\mathbb{Z}_n^* = \{a \in \mathbb{Z} | 1 \leq a \leq n \text{ and } \gcd(a, n) = 1\}$.

7. Lagrange Theorem : If G is a finite group and H is a subgroup of G then $o(H)|o(G)$, Where $o(G)$ is the number of elements of G.

Problems

1. Prove or Disprove the following statements

   (a) Let $(G, *)$ be a group such that $a^2 = e, \forall a \in G$, where e is identity element of G, then $(G, *)$ is cyclic group.

   (b) Let H_1, H_2 are two subgroups of a cyclic group $(G, *)$ then $(H_1 \bigcap H_2, *)$ is always a cyclic subgroup of G.

   (c) Let H_1, H_2 are two subgroups of a cyclic group $(G, *)$ such that $(H_1 \bigcup H_2, *)$ is a subgroup of G then $(H_1 \bigcup H_2, *)$ is cyclic.

   (d) Let $(G, *)$ be a group and center of G is defined as $Z = \{x \in G | xa = ax, \forall a \in G\}$ then Z is a cyclic subgroup of G.

   (e) $(\mathbb{Z}_n, \oplus_n)$ is a cyclic group for any $n \in \mathbb{N}$.

   (f) $(\mathbb{Z}_n, \otimes_n)$ is a cyclic group for any $n \in \mathbb{N}$.

   (g) $(\mathbb{Z}_n^*, \otimes_n)$ is a cyclic group for any $n \in \mathbb{N}$.

   (h) $(\mathbb{Z}_n \setminus \{0\}, \otimes_n)$ is a cyclic group *if and only if* n is prime.

(i) Let H is a subgroup of a group $(G, *)$ then H is cyclic if G is cyclic.

(j) Let G be a cyclic group of order n generated by $a \in G$ then a^i is also a generator of G *if and only if* $\gcd(i, n) = 1$.

(k) Let H, K are two subgroups of a group $(G, *)$ whose orders are relatively prime then $H \bigcap K = \{e\}$.

(l) Let H, K are two subgroups of a group $(G, *)$ of orders p, n respectively, where p is prime, then either $H \bigcap K = \{e\}$ or H is subgroups of a group K.

(m) The elements of finite order in an abelian group G forms a subgroup.

(n) If G is a group of even order then there are exactly an odd number of elements of order 2.

(o) A group G has no proper subgroups if and only if it is a cyclic group of prime order.

(p) There exists a non-abelian group such that each of its proper subgroups is cyclic.

(q) Let H is a subgroup of a group $(G, *)$ then $\forall x \in H$, $x^{-1}Hx$ is a subgroup of G of the same order as that of H.

2. Find all possible sets of generators of the subgroups of orders 3,4, and 12 of $(\mathbb{Z}_{12}, \oplus_{12})$.

3. Calculate the following values.

   (a) $5^{52} \mod 11$

   (b) $7^{41} \mod 12$

   (c) $3^{88} \mod 20$

   (d) $4^{22} \mod 27$

   (e) $9^{96} \mod 19$