MTH 751 Pre-Assignment

(1) If $A \subseteq B$, show that $A \cup B = B$.

(2) Let $A$ be a finite set with $n$ elements. Show that $A$ has $2^n$ number of subsets.

(3) Let $S$ be a finite set and $A(S)$ denote the set of bijections from $S \to S$. Show that if $S$ has $n$ elements $A(S)$ has $n!$ elements.

(4) Let $\circ$ denote composition of functions and $\sigma, \phi, \psi \in A(S)$. Denote the identity map by $i$. Show that
 (a) $\sigma \circ \phi \in A(S)$
 (b) $(\sigma \circ \phi) \circ \psi = \sigma \circ (\phi \circ \psi)$.
 (c) $\sigma \circ i = i \circ \sigma$.
 (d) For every $\sigma \in A(S)$ there exists a $\phi \in A(S)$ such that $\sigma \circ \phi = \phi \circ \sigma$.

(5) Prove that there do not exist integers $a$ and $b$, such that $a^2 + b^2 \equiv 3 \mod 4$. (Hint: Write down the multiplication table for $\mathbb{Z}/4\mathbb{Z}$.

(6) Compute the remainder when $37^{100}$ is divided by 29.

(7) Show that prime factorization of a positive integer is unique.

(8) Given prime factorizations of positive integers $a$ and $b$ write down the g.c.d of $a$ and $b$ in terms of those prime factorizations. Repeat the exercise for the least common multiple of $a$ and $b$. (Hint: First relate g.c.d with l.c.m.)

(9) Let $(a, b)$ denote the g.c.d. of positive integers $a$ and $b$. Show that there exist $m, n \in \mathbb{Z}$ such that $(a, b) = ma + nb$. (Hint: Take the least element of the set of all $\{ma + nb \mid m, n \in Z, ma + nb > 0\}$.)

(10) Let $\mathbb{Z}$ denote the set of integers. Let $p$ be a natural number. Define a relation $\sim$ on $\mathbb{Z}$ as follows; for any $a, b \in \mathbb{Z}$, $a \sim b$ if $n/b - a$. Does $\sim$ define an equivalence relation?

(11) Given a set a $A$, let $R \subset A \times A$ define a equivalence relation. Show that equivalence classes under $R$ give a partition of $A$.

(12) Let $\mathbb{Z}/n\mathbb{Z}$ denote the set of equivalence classes of $\mathbb{Z}$ under a partition defined by $\sim$ (as defined in problem 10). Show that $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under addition defined on the equivalence classes. Is multiplication well defined on $\mathbb{Z}/n\mathbb{Z}$ ? Is $\mathbb{Z}/n\mathbb{Z}$ a group for all $n \in \mathbb{Z}, n \geq 0$?