Assignment I

1. Suppose a, n are positive integers, $1 \leq a \leq n$. Let $d = GCD(a, n)$. Suppose b is a multiple of d. Show that: ☐

   - The equation $ax = b \mod n$ is solvable.
   - If x is one solution, $x + \frac{n}{d}$ is also a solution.
   - The equation has exactly d solutions between 1 and n.
   - For what values of a between 1 and 20 does the equation $ax = 12 \mod 20$ fail to have a solution?

2. Let $\mathcal{S}$ be a set. Let $S_1, S_2, .., S_k$ be non-empty subsets of $\mathcal{S}$. We say $S_1, .., S_k$ forms a *partition* of the set $\mathcal{S}$ if they are disjoint (that is, $S_i \cap S_j = \emptyset$ whenever $i \neq j$) and every element in $\mathcal{S}$ belongs to some (actually exactly one - why?) S_j for some $1 \leq j \leq k$. Given a partition as above, define a relation R on the set S as follows: $R = \{(a, b) \in \mathcal{S} :$ there exists some S_j containing both a and $b\}$. Thus, two elements are related if they belong to the same subset. Show that R is an equivalance relation. (An equivalance relation is one that is reflexive, symmetric and transitive - If you have forgotten the definitions, revise!). ☐

3. Let R be an equivalance relation defined on a set $\mathcal{S}$. For each $a \in \mathcal{S}$, we denote by $R(a)$ the set of all elements to which a is related. That is $R(a) = \{y \in \mathcal{S} : (a, y) \in R\}$. Show that if a, b are distinct elements in $\mathcal{S}$, then either $R(a) = R(b)$ or $R(a) \cap R(b) = \emptyset$. This question and the one above shows that the notions of equivalance relation conincides with the notion of partition of a set. ☐

4. Let n be any positive integer. On the set $\mathbf{Z}$ of integers, define the relation $R = \{(a, b) : a \equiv b \mod n\}$. Show that R is an equivalance relation. How does this relation partition the set $\mathbf{Z}$? ☐

5. Let $(G, +)$ be an Abelian group. Let S be a subgroup. Define the relation R as follows: $R = \{(a, b) \in G : a - b \in S\}$. Show that R is an equivlance relation. When G is $(\mathbf{Z}, +)$, and $S = 4\mathbf{Z}$ (that is S consists of all multiples of 4), describe the tuples in the relation R andthe partioning of $\mathbf{Z}$ defined by this equivalance relation. Repeat the exercise with $G = \mathbf{Z_{10}}$ and $S = \{0, 5\}$. ☐

6. Let S be a subgroup of an an Abelian group $(G, +)$. Let R be the relation: $R = \{(a, b) \in G : a - b \in S\}$. Prove that partion of G defined by R are precisely the **cosets** of G defined by S. ☐

7. Let $\leq$ be a partial order relation on a set A (Revise the definition of partial orders if you have forgotten!) $u \in A$ is an upper bound to $a \in A$ if $a \leq u$. Let S be a (non-empty) subset of A. We define $UB(S) = \{u : u$ is an upper bound to every element in $s\}$. Thus, upper bound of a set consists of those elements u in A such that for every $s \in S$, $s \leq u$. ☐

   - Define the lower bound of two elements and $LB(S)$ in similar manner.
   - In the set of real numbers with the normal ordering $(\mathbf{R}, \leq)$, consider the subset $S = \{a : a^2 < 2\}$. Find $LB(S)$ and $UB(S)$.
   - In the set of vectors in the plane $\mathbf{R^2}$, define the relation $(x, y) \preceq (x', y')$ if $x \leq x'$ and $y \leq y'$. Show that R is partial order. Consider the "square" $S = \{(x, y) : |x| \leq 1, |y| \leq 1\}$. Find $UB(S)$ and $LB(S)$.
   - Is it always true that $UB(S) \cap S = \emptyset$?

8. Let $\leq$ be a partial order relation on a set A. Let S be a (non-empty) subset of A. $l \in S$ is a least element of S if $l \leq s$ for all $s \in S$. Show that S has a least element if and only if $LB(S) \cap S \neq \emptyset$. Show that a set S can have at most one least element. How many elements will be there in $LB(S) \cap S$? Define the notion of greatest element of S in a simlar way. ☐

9. In the set of real numbers with the normal ordering $(\mathbf{R}, \leq)$, consider the subset $S = \{a \in \mathbf{R} : a^2 \leq 2\}$. Does S have a least element? Suppose, instead of reals, we consider the set of rationals with the normal ordering $(\mathbf{Q}, \leq)$. Let S be defined as $S = \{a \in \mathbf{Q} : a^2 \leq 2\}$. Does S have a least element? ☐

10. Let $\leq$ be a partial order relation on a set A. Let S be a (non-empty) subset of A $u \in A$ is the greatest upper bound of S denoted $LUB(S)$ if u is the least element of $UB(S)$. Define $GLB(S)$ similarly. $\square$

11. A partial order $(A, \leq)$ is a lattice if every non-empty **finite** subset S of A has $LUB(S)$ and $GLB(S)$. A is a *complete lattice* if every non-empty subset has $LUB(S)$ and $GLB(S)$. $\square$

    - Show that in $(\mathbf{Q}, \leq)$, the set $S = \{a \in \mathbf{Q} : a^2 < 2\}$ has no $LUB(S)$ or $GLB(S)$. However, show that $(\mathbf{Q}, \leq)$ is a lattice.
    - Show that in $(\mathbf{R}, \leq)$, the set $S = \{a \in \mathbf{R} : a^2 < 2\}$ has $LUB(S)$ and $GLB(S)$. However show that $(\mathbf{R}, \leq)$, though a lattice, is not a complete lattice. If we add two special elements $\pm\infty$ and fix the convention that $LUB(R) = +\infty$ and $GLB(R) = -\infty$, then we get what is known as the *extended real numbers*, which is indeed a complete lattice. The proof of the fact that this system is a complete lattice is beyond the scope of the course.