ASSIGNMENT 2 (DUE ON 13 AUGUST 2021 AT 11:59PM)

MATH2301, SEMESTER 2, 2021

INSTRUCTOR: ASILATA BAPAT

(1) Consider modular addition with the modulus $d = 6$. For each modular number $[x]$, determine whether or not $[x]$ has a multiplicative inverse, and if yes, find the inverse. That is, figure out whether there is some $[y]$ such that $[x] \cdot [y] = [1]$.
(Bonus: Can you find a pattern here? Does a number ever have more than one inverse?)

> *Solution.* There are 6 equivalence classes modulo d, namely $[0], [1], \ldots, [5]$. Note that $[1]\cdot[1] = [1] = [5]\cdot[5]$. None of the other numbers have inverses: you can check this directly, for example note that $[0] \cdot [x] = [0]$ for any $[x]$, and similarly we have $[2] \cdot [1] = [2]$, $[2] \cdot [2] = [4]$, $[2] \cdot [3] = [0]$, $[2] \cdot [4] = [2]$, $[2] \cdot [5] = [4]$, etc.
>
> No number has more than one inverse. Indeed, if $[x] \cdot [y] = [1]$ and $[x] \cdot [z] = [1]$ then we know that $xy = 6n + 1$ and $xz = 6m + 1$, and so $xy - xz = x(y - z) = 6(n - m)$. On the other hand, we know that $yx = 6n + 1$, so multiplying the previous equation by y, we get
> $$(6n + 1)(y - z) = 6(n - m).$$
> Rewrite to see that $(y - z) + 6n(y - z) = 6(n - m)$, or $(y - z) = 6(n - m) - 6n(y - z)$. Since the right hand side is a multiple of 6, we see that $[y] = [z]$.
>
> The pattern is that a number cannot have a multiplicative inverse if it is divisible by any prime that 6 is also divisible by. Note that having an inverse means that $[x] \cdot [y] = [1]$, so that $xy = 6n + 1$, or alternatively, $xy - 6n = 1$ for some n. Now if x is divisible by 2 (or 3), then the left hand side is divisible by 2 (or 3), while the right hand side isn't, and so that equation cannot be true. On the other hand, suppose that $[x]$ does not share any common factor with $[6]$, which means that their greatest common divisor (GCD) equals 1. The Euclid's GCD algorithm (which we haven't talked about in class) says that there must be integers m and n such that $mx + 6n = 1$. If you rewrite this as $mx = 6(-n) + 1$, we see that $[m]$ is an inverse of $[x]$. □

(2) Fix a modulus $d > 1$, and consider the equivalence relation $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid d \mid (x - y)\}$. Let x and y be two arbitrary integers. Show that if $[x] = [y]$, then $[x^2] = [y^2]$.

> *Solution.* Knowing that $[x] = [y]$ means that there is some integer n such that $x = nd + y$. In this case, we have $x^2 = (nd + y)^2 = n^2d^2 + 2ndy + y^2$. Since $n^2d^2 + 2ndy = (n^2d + 2ny)d$ is a multiple of d, we conclude that $[x^2] = [y^2]$. □

(3) Show that if $3x \equiv 5$ modulo 7, then $x \equiv 4$ modulo 7.

> *Solution.* There are many ways to solve this. Here is one approach. If $3x \equiv 5$ modulo 7, then we know that $3x - 5 = 7n$ for some $n \in \mathbb{Z}$. Note that $3 \times 5 = 7 \times 2 + 1$, and so $15x - 25 = 35n$ gives $x + 14x - 25 = 35n$. Rewriting 25 as $25 = 21 + 4$, we see that
> $$x - 4 = 35n - 21 - 14x = 7(5n + 3 - 2x),$$
> which means that $x \equiv 4$ modulo 7. □

(4) For each property listed, find an example of a partial order that has that property, with justification or specific examples as appropriate. Draw its Hasse diagram.
(a) A partial order that is also an equivalence relation.

Date: Due on 13 August 2021 at 11:59pm.

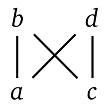
Solution. This is a relation that is reflexive, symmetric, anti-symmetric, and transitive. This means it consists of pairs that lie solely on the diagonal. So for example the relation $\{(a,a),(b,b)\}$ on $S = \{a,b\}$ has this property. $\square$

(b) An element a of a poset is said to be *maximal* there is no element $b \neq a$ such that $a \preceq b$. Find a poset where every element is maximal.

Solution. The previous example also works for this problem: all elements are incomparable so they are all maximal. $\square$

(c) An element a of a poset is said to be the *maximum* element if for every element b, we have $b \preceq a$. Find a poset that has at least one maximal element but no maximum elements.

Solution. Consider the partial order relation on $\{a,b,c,d\}$ specified by $a \preceq b$, $a \preceq d$, $c \preceq b$, $c \preceq d$.



$\square$

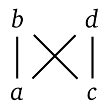
(5) Let $(P, \preceq)$ be a poset and let A be any subset of P. An element $u \in P$ is said to be an *upper bound* for A if for each $a \in A$, we have $a \preceq u$. An element $l \in P$ is said to be a *lower bound* for A if for each $a \in A$, we have $l \preceq a$. Further, an element $u \in P$ is said to be a *least upper bound* (lub) for A if:
- u is an upper bound for A, and
- if $v \in P$ is any upper bound for A, then $u \preceq v$.

Similarly, an element $l \in P$ is said to be a *greatest lower bound* (glb) for A if:
- l is a lower bound for A, and
- if $m \in P$ is any lower bound for A, then $m \preceq l$.

With this background, answer the following.

(a) Draw a Hasse diagram of a poset $(P, \preceq)$ and write down a subset A that has an upper bound, but no least upper bound. Justify briefly.

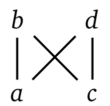
Solution. There are many options. In particular, the following poset works.



We can take $A = \{a,c\}$. Then the elements b and d are the only upper bounds for A, but they are not related to each other so neither of them can be a least upper bound. $\square$

(b) Draw a Hasse diagram of a poset $(P, \preceq)$ and write down a subset A that has a greatest lower bound. Justify briefly.

Solution. There are many options. In particular, the following poset works.



We can take $A = \{a\}$. Then the only lower bound for A is the element a itself, so it is a greatest lower bound. $\square$

(c) Complete the following partial proof of the following statement: "If $(P, \preceq)$ is a poset and $A \subseteq P$ has a least upper bound, then the least upper bound is unique." Write out the third step with full justifications.

(i) Suppose that $A \subseteq P$ has a least upper bound $u \in P$.

(ii) Suppose that $v \in P$ is also a least upper bound of A.

(iii) $\cdots$ $\boxed{\text{Fill this in}}$ $\cdots$

> *Solution.* Since u is a lub for A and v is another upper bound, we have $u \preceq v$. Since v is a lub for A and u is another upper bound, we have $v \preceq u$. The partial order relation is anti-symmetric. So if $u \preceq v$ and $v \preceq u$, then $u = v$. □

(iv) Therefore, $u = v$.

(d) Let S be a finite set and let P be the power set of S with $\subseteq$ as the partial order relation. Let A, B be subsets of S. Find formulas for the lub and glb of $\{A, B\}$. Justify briefly, but you do *not* need to give a formal proof.

> *Solution.* The lub of $\{A, B\}$ is just $A \cup B$. To justify this, first see that $A \subseteq A \cup B$ and $B \subseteq A \cup B$, so the set $A \cup B$ is an upper bound. Now if we have any other upper bound C, it has the property that $A \subseteq C$ and $B \subseteq C$. So every element $a \in A$ is in C and every element $b \in B$ is in C. Any element of $A \cup B$ is either an element of A or an element of B, so we see that $(A \cup B) \subset C$.
>
> The glb of $\{A, B\}$ is just $A \cap B$. To justify this, first see that $A \supseteq A \cap B$ and $B \supseteq A \cap B$, so the set $A \cap B$ is an upper bound. Now if we have any other lower bound C, it has the property that $A \supseteq C$ and $B \supseteq C$. So every element $c \in C$ is both an element of A and an element of B, and thus an element of $A \cap B$. So we see that $(A \cap B) \supset C$. □