

Math 113 Homework 1
Solutions

(1) Do exercise 0.24 in Judson.

(a) We'll show being in either set is equivalent to being in the other:

$$\begin{aligned}
 y \in f(A_1 \cup A_2) &\iff \text{there is } x \in A_1 \cup A_2 \text{ so } f(x) = y \\
 &\iff \begin{array}{l} \text{there is } x_1 \in A_1 \text{ so } f(x_1) = y \\ \text{or} \\ \text{there is } x_2 \in A_1 \text{ so } f(x_2) = y \end{array} \\
 &\iff y \in f(A_1) \text{ or } y \in f(A_2) \\
 &\iff y \in f(A_1) \cup f(A_2)
 \end{aligned}$$

(b) To show the containment, we need to show anything in the lefthand side is also in the right hand side:

$$\begin{aligned}
 y \in f(A_1 \cap A_2) &\iff \text{there is } x \in A_1 \cap A_2 \text{ so } f(x) = y \\
 &\implies \begin{array}{l} \text{there is } x_1 \in A_1 \text{ so } f(x_1) = y \\ \text{and} \\ \text{there is } x_2 \in A_2 \text{ so } f(x_2) = y \end{array} \\
 &\iff y \in f(A_1) \text{ and } y \in f(A_2) \\
 &\iff y \in f(A_1) \cap f(A_2)
 \end{aligned}$$

There is one implication which can't be reversed. This is because x_1 and x_2 might not be equal. So we want a function which is not injective. For example, take $X = Y = \mathbb{Z}$, $f(x) = x^2$, and let A_1 be the positive integers and A_2 be the negative integers. Then $A_1 \cap A_2 = \emptyset$, so $f(A_1 \cap A_2) = \emptyset$. But $f(A_1) = f(A_2) = f(A_1) \cap f(A_2)$ is all positive squares.

(c) Being in either set is equivalent:

$$\begin{aligned}
 x \in f^{-1}(B_1 \cup B_2) &\iff f(x) \in B_1 \cup B_2 \iff f(x) \in B_1 \text{ or } f(x) \in B_2 \\
 &\iff x \in f^{-1}(B_1) \text{ or } x \in f^{-1}(B_2) \\
 &\iff x \in f^{-1}(B_1) \cup f^{-1}(B_2)
 \end{aligned}$$

(d) Being in either set is equivalent:

$$\begin{aligned}
 x \in f^{-1}(B_1 \cap B_2) &\iff f(x) \in B_1 \cap B_2 \iff f(x) \in B_1 \text{ and } f(x) \in B_2 \\
 &\iff x \in f^{-1}(B_1) \text{ and } x \in f^{-1}(B_2) \\
 &\iff x \in f^{-1}(B_1) \cap f^{-1}(B_2)
 \end{aligned}$$

(e) Being in either set is equivalent. For $x \in X$:

$$\begin{aligned}
 x \in f^{-1}(Y \setminus B_1) &\iff f(x) \in Y \setminus B_1 \iff f(x) \notin B_1 \\
 &\iff x \notin f^{-1}(B_1) \iff x \in X \setminus f^{-1}(B_1)
 \end{aligned}$$

(2) (a) Show that relation \neq on the integers is symmetric, but neither reflexive or transitive.

If $x \neq y$ then $y \neq x$, so \neq is symmetric. Since $0 = 0$, \neq is not reflexive. Also $0 \neq 1$ and $1 \neq 0$ but $0 = 0$, so \neq is not transitive.

- (b) Given an example of a relation which is symmetric and transitive, but not reflexive.

In order to break reflexivity, we need to have some a so that $a \not\sim a$. However, we have a problem if $a \sim b$ for some other b , because then $b \sim a$ by symmetry, and we would get $a \sim a$ by transitivity. So we need to make sure a isn't related to anything. For example, take the relation on the integers define by: $a \sim b$ if a and b are both nonzero. This relation is symmetric and transitive but $0 \not\sim 0$.

- (3) Suppose X , Y , and Z are sets, and $f : X \rightarrow Y$, $g : X \rightarrow Y$, $h : Y \rightarrow Z$, and $i : Y \rightarrow Z$ are functions.

- (a) Prove that if h is injective and $h \circ f = h \circ g$, then $f = g$.

To show that $f = g$, we need to prove that for any $x \in X$, $f(x) = g(x)$. As $h \circ f = h \circ g$, we know $h(f(x)) = h(g(x))$. Since h is injective, we then know that $f(x) = g(x)$.

- (b) Prove that if f is surjective and $h \circ f = i \circ f$, then $h = i$.

To show that $h = i$, we need to prove that for any $y \in Y$, $h(y) = i(y)$. Since f is surjective, we know there is some $x \in X$ so that $f(x) = y$. Because $h \circ f = i \circ f$, we get that $h(y) = h(f(x)) = i(f(x)) = i(y)$.

- (4) Given any function $g : X \rightarrow Y$, we can define a relation on X by

$$a \sim_g b \text{ if } g(a) = g(b)$$

- (a) Prove that \sim_g is always an equivalence relation.

We need to verify that \sim_g is reflexive, symmetric, and transitive. For any $x \in X$, $g(x) = g(x)$ so $x \sim_g x$, giving us reflexivity. For $x_1, x_2 \in X$, if $x_1 \sim_g x_2$, then $g(x_1) = g(x_2)$, so also $x_2 \sim_g x_1$, i.e. \sim_g is symmetric. Finally, if $x_1, x_2, x_3 \in X$ and $x_1 \sim_g x_2$ and $x_2 \sim_g x_3$, then we know $g(x_1) = g(x_2) = g(x_3)$. So $x_1 \sim_g x_3$ and \sim_g is transitive.

- (b) Given a set Z , and an equivalence relation \bowtie on Z , we can define a function $f : Z \rightarrow$ equivalence classes of \bowtie by

$$f(x) = [x]$$

- (i) Prove that f is actually a function.

Since equivalence classes for a partition, we know $f(x)$ has exactly one value for each $x \in X$.

- (ii) Prove that f is surjective.

If A is any equivalence class of \bowtie , by definition A is not empty. Let $a \in A$. Then $f(a) = [a] = A$. So every equivalence class is hit by f . I.e. f is surjective.

(iii) Prove that f is injective if and only if \bowtie is equality.

To prove one direction, assume that f is injective. Let x_1, x_2 be arbitrary elements of X . If $x_1 \bowtie x_2$. Then $f(x_1) = [x_1] = [x_2] = f(x_2)$. By injectivity of f , $x_1 = x_2$. Also, $x_1 \bowtie x_1$ since every equivalence relation is reflexive. So \bowtie is just equality.

Now to prove the other way, assume that \bowtie is equality. Suppose that $f(x_1) = f(x_2)$. Then $[x_1] = [x_2]$. So $x_1 \bowtie x_2$, i.e. $x_1 = x_2$.

(iv) Prove that \sim_f and \bowtie are the same equivalence relation. So any equivalence relation comes from a function in this way.

For any $x_1, x_2 \in X$:

$$x_1 \sim_f x_2 \iff f(x_1) = f(x_2) \iff [x_1] = [x_2] \iff x_1 \bowtie x_2$$

So \sim_f and \bowtie are the same.

(5) Prove by induction that $n^5 - n$ is always divisible by 5.

Base Case: If $n = 0$, $n^5 - n = 0^5 - 0 = 0$ which is divisible by 5.

Inductive step: Assume $5 \mid k^5 - k$. Now consider the case of $k + 1$:

$$(k+1)^5 - (k+1) = k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1 - k - 1 = 5(k^4 + 2k^3 + 2k^2 + k) + (k^5 - k)$$

By our inductive assumption, this must also be divisible by 5.

And by induction $5 \mid n^5 - n$ for all integers $n \geq 0$.

(6) Do exercise 1.12 in Judson.

We will prove by induction that a set with n elements has a power set with 2^n elements.

Base Case $n = 0$: There's only one set with zero elements, \emptyset . It has one subset, itself. $2^0 = 1$, so the base case holds.

Assume every set of size k has exactly 2^k subsets. Consider a set X of size $k + 1$. Let x be an element of X . By assumption $X \setminus \{x\}$ has 2^k elements. For each subset of X , either x is included or not. The subsets of X that include x are the same as the subsets of $X \setminus \{x\}$ with x added. The subsets of X without x are just the subsets of $X \setminus \{x\}$. So there are $2^k + 2^k = 2^{k+1}$ subsets of X in total. This completes the induction and the proof.

(7) Let p_1, \dots, p_k be distinct primes, and $a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k$ be positive integers. Let $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k}$ and $m = p_1^{b_1} \cdot p_2^{b_2} \cdot \dots \cdot p_k^{b_k}$. Compute $\gcd(n, m)$.

We know that $\gcd(n, m)$ has to have a prime factorization. The only primes that can divide $\gcd(n, m)$ are those that divide both n and m . Similarly $p_i^{c_i}$ can only divide $\gcd(n, m)$ if it divides both n and m , so $c_i \leq a_i, b_i$. So $\gcd(n, m)$ must be $p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdot \dots \cdot p_k^{\min(a_k, b_k)}$ since it divides n and m and nothing greater can.

(8) Do exercise 1.27 in Judson.

Since $\gcd(a, b) = 1$, there are s and t so that $sa + bt = 1$. So $c = c(sa + bt) = a(sc) + bc(t)$. Since a divides a and a divides bc , it must divide $a(sc) + bc(t) = c$.

(9) Do exercise 1.30 in Judson.

First we will prove a lemma similar to the one we proved in class:

Every positive integer of the form $4n - 1$ is divisible by a prime of the same form.

Proof: We'll use the well ordering principle on

$$S = \{4n - 1 : 4n - 1 > 0 \text{ and no prime of the form } 4k - 1 \text{ divides } 4n - 1\}$$

Consider an arbitrary $4m - 1 \in S$. $4m - 1$ cannot be prime because it is in S and divides itself. Also $4m - 1 > 1$. So $4m - 1 = ab$ for some $a, b > 1$. Since $4m - 1$ is odd, both a and b are odd. It is not possible for both a and b to be of the form $4i + 1$, because then $4m - 1$ would also be of that form. So one of a and b is of the form $4i - 1$. Any prime that divides a or b also divides $4m - 1$. So one of a and b must be in S . So something smaller than $4m - 1$ is in S . Since $4m - 1$ was arbitrary, S has no least element. So by the well ordering principle, S must be empty and the lemma is true.

Now we can finish the problem: Consider any finite list of primes of the form $4i - 1$, call them p_1, p_2, \dots, p_n . Let $a = p_1 \cdot p_2 \cdot \dots \cdot p_n$. If a is of the form $4i - 1$, put $q = a + 4$. Otherwise a is of the form $4i + 1$, so put $q = a + 2$. In either case, q is of the form $4i - 1$ and none of p_1, p_2, \dots, p_n divide q . By the lemma, some prime of the form $4i - 1$ divides q . So some prime of the form $4i - 1$ is absent from the list. So no finite list of primes can have all the primes of the form $4i - 1$. There must be infinitely many such primes.