02/26/2025: Equivalence Relations

CSCI 246: Discrete Structures

Textbook reference: Sec 15, Scheinerman

Graded Quiz Pickup

Quizzes are in the front of the room, grouped into four bins (A-G, H-L, M-R, S-Z) by last name. The quizzes are upside down with your last name on the back. Come find yours before, during, or after class. Only turn the quiz over if it's yours.

Announcements

This Friday's problem quiz will cover relations (including equivalence relations) - see slide decks from 2/19, 2/24, and 2/26.

Next Friday's problem quiz will cover partitions and functions

Today's Agenda

- Reading quiz (10 mins)
- Mini-lecture ($\approx$ 20 mins)
- Group exercises ($\approx$ 15 mins)

Reading Quiz (Equivalence Relations) (Extra Credit)

Prove the theorem below.

Theorem

Let n be a positive integer. Congruence modulo n is an equivalence relation on the set of integers.

Definition

Let n be a positive integer. We say that integers x and y are **congruent modulo n**, and we write

$$x \equiv y \pmod{n}$$

if $n|(x-y)$.

Solution to reading quiz

Solution to reading quiz

We verify the three properties of an equivalence relationship below.

- *Reflexivity*:

Solution to reading quiz

We verify the three properties of an equivalence relationship below.

- *Reflexivity*: We need to check xRx. That is, we need to check $n|(x-x)$. In other words, we need to check $n|0$. By definition of divisibility, we need to check that there is an integer c such that $nc = 0$. This is satisfied by setting $c = 0$. ✓
- *Symmetry*:

Solution to reading quiz

We verify the three properties of an equivalence relationship below.

- *Reflexivity*: We need to check xRx. That is, we need to check $n|(x-x)$. In other words, we need to check $n|0$. By definition of divisibility, we need to check that there is an integer c such that $nc = 0$. This is satisfied by setting $c = 0$. ✓
- *Symmetry*: We need to check that if xRy , then yRx. In other words, we need to check that if $n|(x-y)$, then $n|(y-x)$. Let $n|(x-y)$. Then there is an integer c such that $nc = x-y$. Hence $n(-c) = y-x$. So $n|(y-x)$. ✓
- *Transitivity*:

Solution to reading quiz

We verify the three properties of an equivalence relationship below.

- *Reflexivity*: We need to check xRx. That is, we need to check $n|(x-x)$. In other words, we need to check $n|0$. By definition of divisibility, we need to check that there is an integer c such that $nc = 0$. This is satisfied by setting $c = 0$. ✓
- *Symmetry*: We need to check that if xRy , then yRx. In other words, we need to check that if $n|(x-y)$, then $n|(y-x)$. Let $n|(x-y)$. Then there is an integer c such that $nc = x-y$. Hence $n(-c) = y-x$. So $n|(y-x)$. ✓
- *Transitivity*: We need to check that if xRy and yRz , then xRz. That is, we need to check that if $n|(x-y)$ and $n|(y-z)$, then $n|(x-z)$. By assumption, there are integers c and d such that $nc = (x-y)$ and $nd = (y-z)$. Now we write

  $$x - z = (x-y) + (y-z) = nc + nd = n(c+d).$$

  Since $c+d$ is an integer, clearly $n|x-z$. ✓

Remark

For intuition, note that $x \equiv y \pmod{n}$ if x and y have the same remainder after dividing by n. For example, $4 \equiv 1 \pmod{3}$.

Definition

Let R be an equivalence relation on a set A and let $a \in A$. The *equivalence class* of a, denoted $[a]$, is the set of all elements of A related (by R) to a. That is,

$$[a] = \{x \in A : xRa\}$$

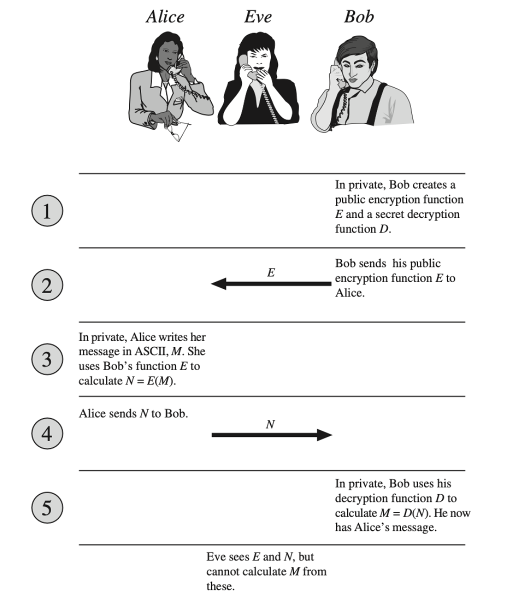
Example

The integers can be partitioned into the following equivalence classes

$$[0] = \{\dots, -6, -3, 0, 3, 6, \dots\}$$
$$[1] = \{\dots, -5, -2, 1, 4, 7, \dots\}$$
$$[2] = \{\dots, -4, -1, 2, 5, 8, \dots\}$$

under the relation of congruence mod 3.

Application: Public-Key Cryptography



Feedback on Monday’s Quiz

Scores On Reading Quiz (Relations)

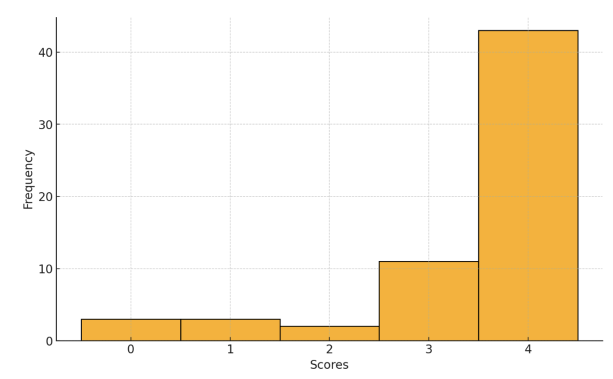


Figure 1: Median Score = 4/4 (100%)

Rubric. 1 point for each subquestion if correct.

Q&A On Previous Group Exercises

Group exercises

aaron.loomis: 11
adam.wyszynski: 6
alexander.goetz: 19
alexander.knutson: 8
anthony.mann: 14
blake.leone: 10
bridger.voss: 9
caitlin.hermanson: 20
cameron.wittrock: 16
carsten.brooks: 15
carver.wambold: 6
colter.huber: 17
conner.reed1: 22
connor.graville: 7
connor.mizner: 3
connor.yetter: 1
delaney.rubb: 8
derek.price4: 19
devon.maurer: 14
emmeri.grooms: 13
erik.moore3: 3
ethan.johnson18: 4
evan.barth: 18
evan.schoening: 9
griffin.short: 17
jack.fry: 3
jacob.ketola: 18
jacob.ruiz1: 7
jacob.shepherd1: 10
jada.zorn: 22
jakob.kominsky: 12
james.brubaker: 22
jeremiah.mackey: 5
jett.girard: 21
john.fotheringham: 2
jonas.zeiler: 14
joseph.mergenthaler: 11
joseph.triem: 21
julia.larsen: 10
justice.mosso: 6
kaden.price: 5
lucas.jones6: 5
luka.derry: 18
luke.donaldson1: 2
lynsey.read: 1
mason.barnocky: 20
matthew.nagel: 16
micaylyn.parker: 2
michael.oswald: 9
nolan.scott1: 15
owen.obrien: 13
pendleton.johnston: 7
peter.buckley1: 19
peyton.trigg: 21
reid.pickert: 11
ryan.barrett2: 12
samuel.hemmen: 16
samuel.mosier: 1
samuel.rollins: 15
sarah.periolat: 17
timothy.true: 20
tristan.nogacki: 4
tyler.broesel: 12
william.elder1: 13
yebin.wallace: 4
zeke.baumann: 8

Group exercises

1. Which of the following are equivalence relations?

   a. $\mid$ on $\mathbb{Z}$.
   b. $\leq$ on $\mathbb{Z}$.
   c. Is-an-angram-of on the set of English words. (For instance, `STOP` is an anagram of `POTS` because we can form one from the other by rearranging its letters.)
   d. $R = \{(1,2),(2,3),(3,1)\}$ on the set $\{1,2,3\}$.
   e. $\{1,2,3\} \times \{1,2,3\}$ on the set $\{1,2,3\}$.
   f. $\{1,2,3\} \times \{1,2,3\}$ on the set $\{1,2,3,4\}$.

2. For each equivalence relation below, find the requested equivalence class(es).

   a. $R = \{(1,1),(1,2),(2,1),(2,2),(3,3),(4,4)\}$ on $\{1,2,3,4\}$. Find $[1],[2],[3],[4]$
   b. R is has-the-same-tens-digit on the set $\{x \in \mathbb{Z} : 100 < x < 200\}$. Find $[123]$.
   c. R is has-the-same-parents-as on the set of all human beings. Find [you].
   d. R is has-the-same-size-as on $2^{\{1,2,3,4,5\}}$. Find $[\{1,3\}]$.

3. Prove Proposition 15.11: Let R be an equivalence relation on the set A and let $a, x, y \in A$. If $x, y \in [a]$, then xRy.

Solution to group exercise #1

Problem. Which of the following are equivalence relations?

a. $|$ on $\mathbb{Z}$.

b. $\leq$ on $\mathbb{Z}$.

c. Is-an-angram-of on the set of English words. (For instance, STOP is an anagram of POTS because we can form one from the other by rearranging its letters.)

d. $R = \{(1,2),(2,3),(3,1)\}$ on the set $\{1,2,3\}$.

e. $\{1,2,3\} \times \{1,2,3\}$ on the set $\{1,2,3\}$.

f. $\{1,2,3\} \times \{1,2,3\}$ on the set $\{1,2,3,4\}$.

Solution.

a. No, because the relation is not symmetric. For example, $3R6$ but $6\not R3$.

b. No, because the relation is not symmetric. For example, $3R4$ but $4\not R3$.

c. Yes.

d. No, because the relation is not transitive. In particular, we have $1R2$ and $2R3$, but $1\not R3$.

e. Yes.

f. No, because the relation is not reflexive. In particular, $4\not R4$.

Solution to group exercise #2

Problem. For each equivalence relation below, find the requested equivalence class(es).

a. $R = \{(1,1),(1,2),(2,1),(2,2),(3,3),(4,4)\}$ on $\{1,2,3,4\}$. Find $[1],[2],[3],[4]$

b. R is has-the-same-tens-digit on the set $\{x \in \mathbb{Z} : 100 < x < 200\}$. Find [123].

c. R is has-the-same-parents-as on the set of all human beings. Find [you].

d. R is has-the-same-size-as on $2^{\{1,2,3,4,5\}}$. Find $[\{1,3\}]$.

Solution.

a. We have $[1] = [2] = \{1,2\}$, $[3] = \{3\}$, and $[4] = \{4\}$.

b. We have $[123] = \{120, 121, 122, 123, 124, 125, 126, 127, 128, 129\}$.

c. The answer depends on who's answering. I have one sister named Rachael, so for me, [me] = {me, Rachael}.

d. We have

$$[\{1,3\}] = \Big\{\{1,2\},\{1,3\},\{1,4\},\{1,5\},\{2,3\},\{2,4\},\{2,5\},\{3,4\},\{3,5\},\{4,5\}\Big\}.$$

Solution to group exercise #3

Problem. Prove Proposition 15.11: Let R be an equivalence relation on the set A and let $a, x, y \in A$. If $x, y \in [a]$, then xRy.

Solution.. By the definition of equivalence classes (Scheinerman Definition 15.6), we have

$$[a] = \{x \in A : xRa\}.$$

Now by assumption, $x \in [a]$, so we have xRa. Similarly, by assumption, $y \in [a]$, so we have yRa. Since R is an equivalence relation, it is symmetric, and so $yRa \implies aRy$. Now we have xRa and aRy, so by transitivity (which holds since R is an equivalence relation), xRy.