CSE 20
DISCRETE MATH

SPRING 2016

http://cseweb.ucsd.edu/classes/sp16/cse20-ac/

Today's learning goals

- Determine and prove whether a given binary relation is
  - symmetric
  - antisymmetric
  - reflexive
  - transitive
- Represent equivalence relations as partitions and vice versa
- Define and use the congruence modulo m equivalence relation

Reminders

Office hours after class, outside CENTER101

Tomorrow: Last HW due **Thursday:** Review (in class + evening session)

Final exam Saturday 8am-11am in usual lecture room.

- See Piazza for seat assignment
- Practice exam, review session times, extra office hours

Also: CAPE & TA evals are out - please fill out!

Equivalence relations

Rosen p. 608

Two formulations

A relation R on set S is an **equivalence relation** if it is **reflexive**, **symmetric**, and **transitive**.

x R y iff x and y are "similar"

Partition S into **equivalence classes**, each of which consists of "similar" elements: collection of **disjoint**, **nonempty** subsets that have S as their **union**

x,y both in A_i iff x and y are "similar"

Equivalence relations on strings

each of R_1, R_2, R_3 is a different relation

Which of the following binary relations on {0,1}* are equivalence relations?

$\forall x (xRx)$ Refl $\quad \forall x \forall y (xRy \rightarrow yRx)$ Symm $\quad \forall x \forall y \forall z ([xRy \wedge yRz] \rightarrow xRz)$ Transitive

A. u R_1 v iff |u| = |v| ✓ ✓ ✓

B. u R_2 v iff the first bit of u is not equal to the first bit of v ✗ ✗ ✗

C. u R_3 v iff u is the reverse of v ✗ ✓ ✗

D. More than one of the above

E. None of the above

How to prove?

Equivalence relations

Rosen p. 608

Two formulations

A relation R on set S is an **equivalence relation** if it is **reflexive**, **symmetric**, and **transitive**.

x R y iff x and y are "similar"

Partition S into **equivalence classes**, each of which consists of "similar" elements: collection of **disjoint**, **nonempty** subsets that have S as their **union**

x,y both in A_i iff x and y are "similar"

Equivalence classes

Rosen p. 612

Given an equivalence relation R on set S, for a in S,

$$[a] = \{ x : a \, R \, x \}$$

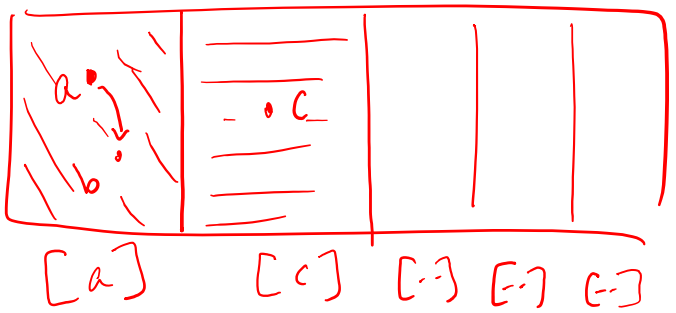
collection of elements in universe similar to a

Theorem 1: Let R be an equivalence relation on a set A. For elements a,b of A

(a) a R b iff

(b) [a] = [b] iff

(c) [a] ∩ [b] is nonempty.



The example

Rosen p. 240

For a,b in **Z** and m in **Z⁺** we say **a is congruent to b mod m** iff

$m \mid (a-b)$

$\exists q(a - b = qm)$

i.e.

and in this case, we write

$a \equiv b \pmod{m}$

Which of the following is true?

A. $5 \equiv 10 \pmod{3}$

B. $5 \equiv 1 \pmod{3}$

C. $5 \equiv 3 \pmod{3}$

D. $5 \equiv -1 \pmod{3}$

E. None of the above.

The example

Rosen p. 240

Claim: Congruence mod m is an equivalence relation

Proof:

Fix m

WTS $\forall x \forall y \forall z \left([x \equiv y \bmod m \wedge y \equiv z \bmod m] \rightarrow x \equiv z \bmod m \right)$

A *Reflexive?*

B *Symmetric?*

C *Transitive?*

Let $x, y, z \in \mathbb{Z}$

Assume ① $x \equiv y \bmod m$ i.e. there's $a \in \mathbb{Z}$ s.t. $x - y = am$

② $y \equiv z \bmod m$ i.e. there's $b \in \mathbb{Z}$ s.t. $y - z = bm$

WTS $x \equiv z \bmod m$ i.e. WTS $m \mid x - z$

$x - z = x - y + y - z = (x - y) + (y - z) = am + bm$

$= (a+b)m$ since $a+b \in \mathbb{Z}$, $m \mid x - z$ by ① and ②

The example

Rosen p. 240

Claim: Congruence mod m is an equivalence relation

Equivalence classes $[a]_R = \{ s : a \, R \, s \}$

What partition of the integers is associated with this equivalence relation?

E.g. m=6

$[0]_6 = \{ s : 0 \equiv s \pmod 6 \}$

{0, 6, 12, 18, 24, …}
{1, 7, 13, 19, 25, …}
{2, 8, 14, 20, 26, …}
{3, 9, 15, 21, 27, …}
{4, 10, 16, 22, 28, …}
{5, 11, 17, 23, 29, …}

6 classes (each of infinite size)

Arithmetic modulo *m*

Rosen p. 242-243

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$

Modular addition and multiplication are well-defined on equivalence classes!

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Application 1: Last digit

What's the last digit of 2016^{2016}?

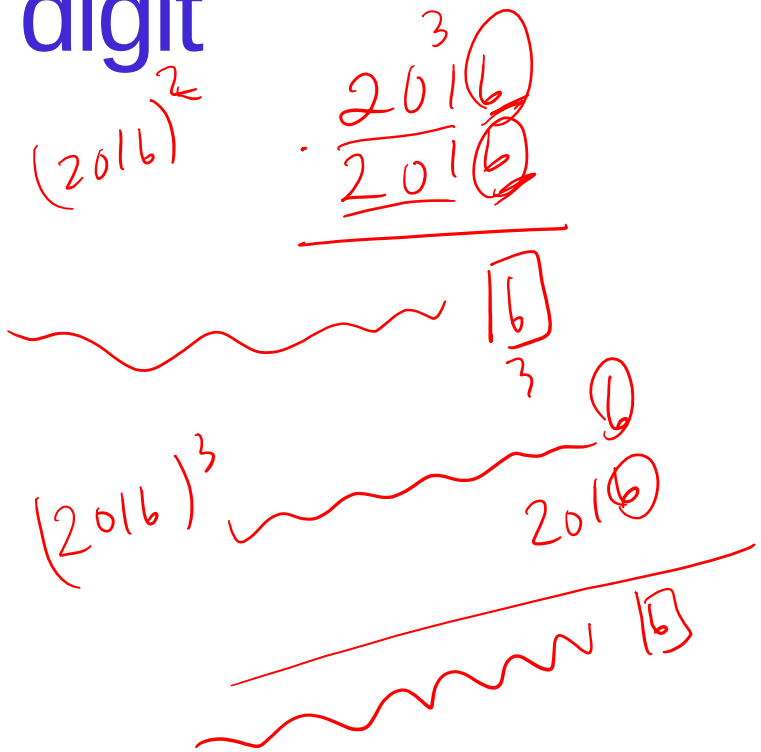
A. 1

B. 6

C. 2

D. 0

E. Can't tell without a calculator.

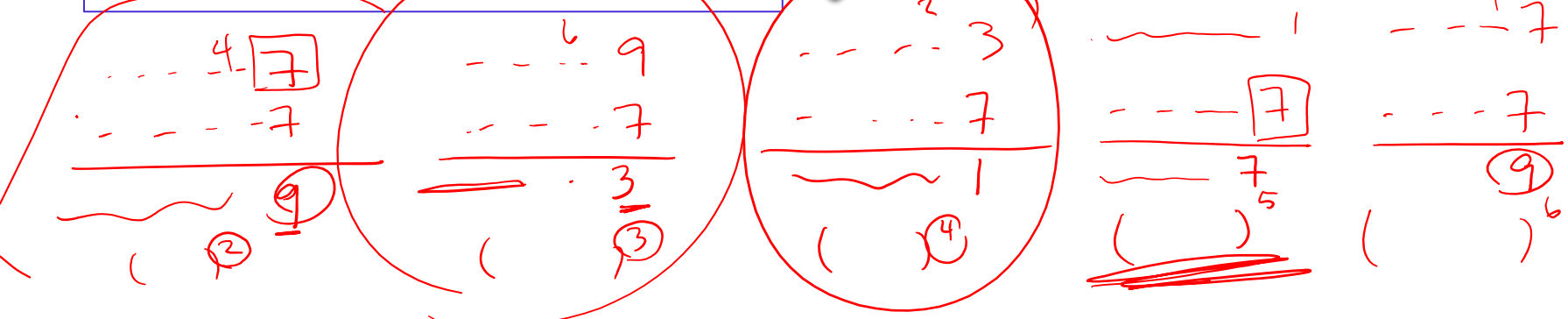


Application 1: Last digit

What's the last digit of 1234567^{890}?

A. 1
B. 7
C. 3
D. 9
E. Can't tell without a calculator

Last digit of decimal representation of n is n **mod** 10



Modular operations

We saw that, for all integers a,b and all positive integers m,

$$(a+b) \textbf{ mod } m = ((a \textbf{ mod } m) + (b \textbf{ mod } m)) \textbf{ mod } m$$

$$ab \textbf{ mod } m = ((a \textbf{ mod } m) (b \textbf{ mod } m)) \textbf{ mod } m$$

Which of the following is also true?

A. $(a-b) \textbf{ mod } m = ((a \textbf{ mod } m) - (b \textbf{ mod } m)) \textbf{ mod } m$

B. $(a/b) \textbf{ mod } m = ((a \textbf{ mod } m) / (b \textbf{ mod } m)) \textbf{ mod } m$

C. $a^b \textbf{ mod } m = ((a \textbf{ mod } m)^{(b \textbf{ mod } m)}) \textbf{ mod } m$

D. More than one of the above.

E. None of the above.

Modular operations

(a-b) **mod** m = ((a **mod** m) - (b **mod** m)) **mod** m

True :

(-b) mod m = (m-b) mod m

(a/b) **mod** m = ((a **mod** m) / (b **mod** m)) **mod** m

False :

Counterexample: a = 16, b = 8, m = 10

a^b **mod** m = ((a **mod** m)$^{(b \textbf{ mod } m)}$) **mod** m

False :

Counterexample: a = 2, b= 10, m = 10

Application 2: Proof by cases

Claim: The square of each integer is either divisible by 4 or has remainder 1 upon division by 4.

Proof:

There are 4 possible values for rem. upon div by 4. Consider each of these cases

Let n be int.

Case ②: $n \bmod 4 = 1$ i.e. there's $q \in \mathbb{Z}$

$n = 4q+1$

$n^2 = (4q+1)(4q+1) = 16q^2 + 8q + 1$

n^2?

so $n^2 \bmod 4 = 1$ ☺

Repeat for Case ③ $n \bmod 4 = 2$ ④ $n \bmod 4 = 3$...

Induction?

Contradiction?

Exhaustive?

Application 2: Proof by cases

Claim: The square of each integer is either divisible by 4 or has remainder 1 upon division by 4.

Proof: Let n be an integer and consider its remainder upon division by r.

Four cases: remainder is 0, 1, 2, or 3.

…

Application 3: Pseudorandom generators

Rosen p. 288

$$x_{n+1} = (ax_n + c) \textbf{ mod } m$$

Parameters:

- modulus m
- multiplier a (2 <= a < m)
- increment c (0 <= c < m)
- seed x_0 (0 <= x_0 < m)

What's the maximum number of terms before the sequence starts to repeat?

A. m
B. a
C. c
D. x_0
E. Depends on the parameters; maybe never!

Application 3: Pseudorandom generators

$$x_{n+1} = (ax_n + c) \textbf{ mod } m$$

Parameters:

- modulus m
- multiplier a (2 <= a < m)
- increment c (0 <= c < m)
- seed x_0 (0 <= x_0 < m)

m=8, a=5, c=1, x_0=1 — 1, 6, 7, 4, 5, 2, 3, 0, 1, 6, 7, 4, 5, 2, 3, …

m=8, a=5, c=4, x_0=1 — 1, 1, 1, 1, 1, …

Application 4: Cryptography

Rosen p. 294

- Substitution ciper — modular addition
- RSA — modular exponentiation

f(p) = (p + 4) **mod** 26. Decrypt "07 23 09".

A. ABC
B. HI!
C. SUPERB
D. 03 19 02
E. None of the above

Thursday: review

1. Algorithms
2. Number systems and integer operations
3. Propositional Logic
4. Predicates & Quantifiers
5. Proof strategies
6. Sets
7. Induction & Recursion
8. Functions & Cardinalities of sets
9. Binary relations