CSE 20
DISCRETE MATH

WINTER 2016

http://cseweb.ucsd.edu/classes/wi16/cse20-ab/

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

Thursday: review class

Thursday: HW8 due

Final exam next week: check website for

- time, location, seat assignment
- practice exam, review session times, extra office hours

The example

Rosen p. 240

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

$$m \mid (a-b)$$

i.e.

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

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:

Reflexive?

Symmetric?

Transitive?

The example

Rosen p. 240

Claim: Congruence mod m is an equivalence relation

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

E.g. m=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, …}

Equivalence classes

Rosen p. 612

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

(a) a R b iff

(b) [a] = [b] iff

(c) [a] ∩ [b] is nonempty.

Arithmetic modulo *m*

Rosen p. 242-243

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

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

+	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,

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

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

Which of the following is also true?

A. $(a-b) \bmod m = ((a \bmod m) - (b \bmod m)) \bmod m$
B. $(a/b) \bmod m = ((a \bmod m) / (b \bmod m)) \bmod m$
C. $a^b \bmod m = ((a \bmod m)^{(b \bmod m)}) \bmod m$
D. More than one of the above.
E. None of the above.

Modular operations

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

$(-b) \bmod m = (m-b) \bmod m$

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

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

$a^b \bmod m = ((a \bmod m)^{(b \bmod m)}) \bmod m$

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:

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