

# CSE 20

# DISCRETE MATH

---

Fall 2017

<http://cseweb.ucsd.edu/classes/fa17/cse20-ab/>

# Today's learning goals

- Define and use the congruence modulo  $m$  equivalence relation
- Apply modular arithmetic to solve problems
  - new proof strategies
  - simplify computations
  - memory indexing (hash functions)
  - cryptography (Diffie-Hellman key exchange)
  - pseudo-random number generation

# Equivalence relations

*Rosen p. 608*

*Two formulations*

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

$x R y$  iff  $x$  and  $y$  are "similar"

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

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

# Relation on a set A

*Rosen pp 576-578*

A relation R is called

**reflexive** iff  $\forall a( (a, a) \in R )$

**symmetric** iff  $\forall a \forall b( (a, b) \in R \rightarrow (b, a) \in R )$

**transitive** iff  $\forall a \forall b \forall c( [(a, b) \in R \wedge (b, c) \in R] \rightarrow (a, c) \in R )$

Given an equivalence relation R on set A, for a in A, the **equivalence of class** of a is

$$[a]_R = \{s \mid (a,s) \text{ is in } R\}$$

# \*The\* example

Rosen p. 240

For  $a, b$  in  $\mathbf{Z}$  and  $m$  in  $\mathbf{Z}^+$  we say  **$a$  is congruent to  $b$  mod  $m$**

iff  $a \bmod m = b \bmod m$  \*

iff  $m \mid (a-b)$

i.e.  $\exists q(a - b = qm)$

and in this case, we write

$a \equiv b \pmod{m}$   
notation

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?*

} on your own

# \*The\* example

Rosen p. 240

**Claim:** Congruence mod  $m$  is an equivalence relation

**Congruence classes:**  $[a]_m = \{s \mid (a,s) \text{ is in } R\} = \{s \mid a \bmod m = s \bmod m\}$

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

E.g.  $m=6$

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

$$\{0, 6, 12, 18, 24, \dots\} = [-6]_6$$

$$\{3, 9, 15, 21, 27, \dots\} = [-3]_6$$

$$\{1, 7, 13, 19, 25, \dots\} = [-5]_6$$

$$\{4, 10, 16, 22, 28, \dots\} = [-2]_6$$

$$\{2, 8, 14, 20, 26, \dots\} = [-4]_6$$

$$\{5, 11, 17, 23, 29, \dots\} = [-1]_6$$

# Application 1: Proof by cases

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

$\forall n$

$$\left( n^2 \bmod 4 = 0 \vee n^2 \bmod 4 = 1 \right)$$

Universe:  $\mathbb{Z}$

**Proof:**

Induction?

Contradiction?

Exhaustive?

Proof by cases

evens

odds

Proof by cases

$n \bmod 4 = 0$

$n \bmod 4 = 1$

$n \bmod 4 = 2$

$n \bmod 4 = 3$



# Application 1: 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 4.

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

...

# Arithmetic modulo $m$

Rosen p. 242-243

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

$$\boxed{ab} \bmod m = ((a \bmod m) (b \bmod m)) \bmod m$$

in proof case ①  
 $n \bmod 4 = 0$

$$\begin{aligned} n^2 \bmod 4 &= ((n \bmod 4)(n \bmod 4)) \bmod 4 \\ &\stackrel{\text{by assumption}}{=} (0 \cdot 0) \bmod 4 \\ &= 0 \bmod 4 = 0 \end{aligned}$$

# 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!*

<del>+</del>	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



# 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

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

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

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

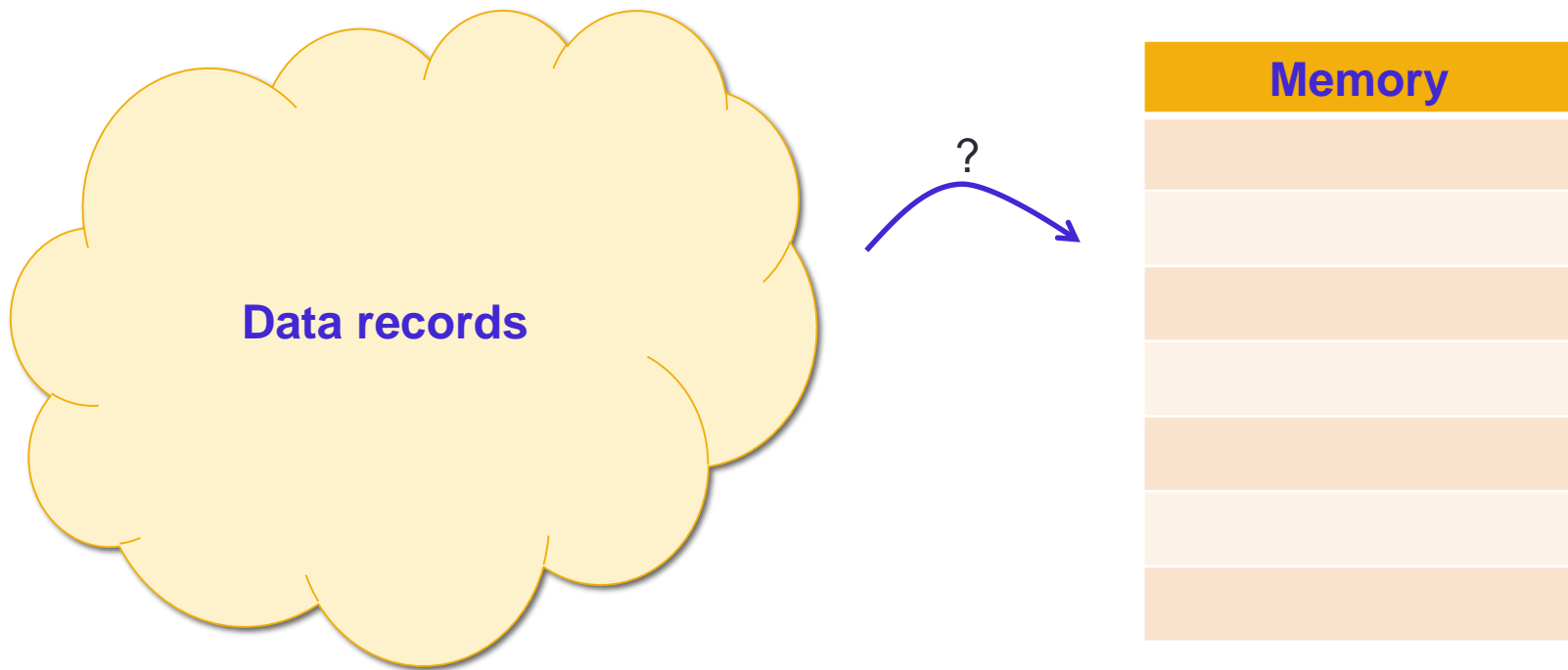
*Counterexample:  $a = 16, b = 8, m = 10$*

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

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

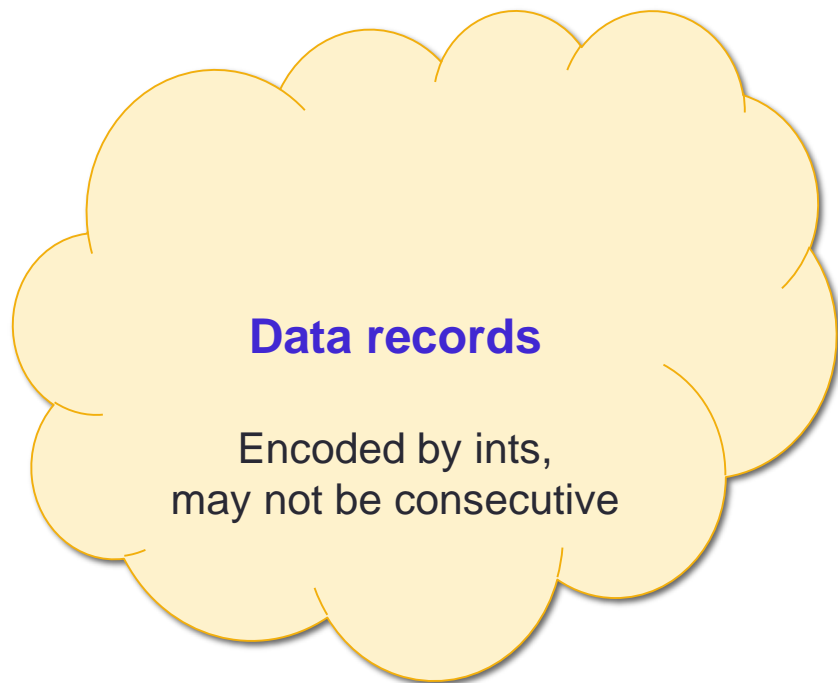
# Application 3: hashing

*Rosen Sec 4.5 p. 287*

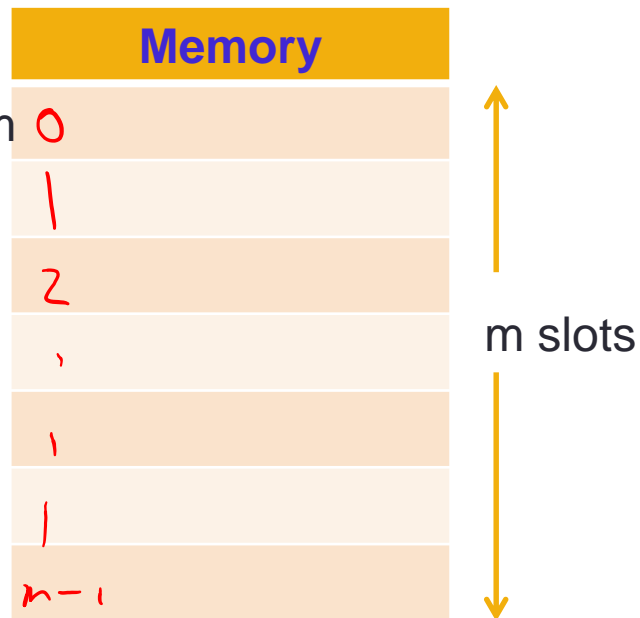


# Application 3: hashing

Rosen Sec 4.5 p. 287



$$h(k) = k \bmod m$$

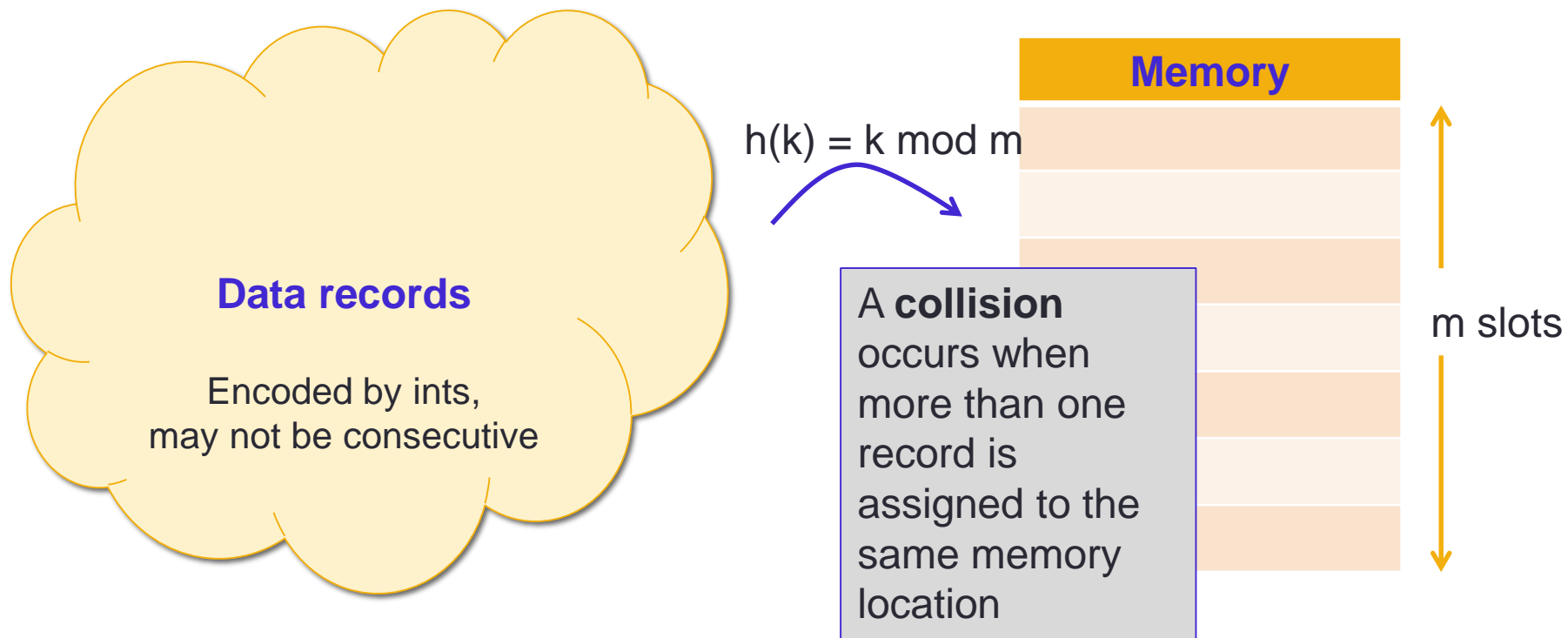


Well-defined? Onto? One-to-one?



# Application 3: hashing

*Rosen Sec 4.5 p. 287*



# Application 4: key exchange

*Rosen Sec 4.6, p. 302*



# Application 4: key exchange

*Rosen Sec 4.6, p. 302*

Sender starts with

- Public key, public prime  $a, p$
- Private key  $k_1$

Receiver starts with

- Public key, public prime  $a, p$
- Own private key  $k_2$

Idea: exchange information so that sender and receiver will have shared **key** (number) but no-one looking at messages will be able to decode them without knowing either or both of  $k_1, k_2$

# Application 4: key exchange

*Rosen Sec 4.6, p. 302*

## Basic assumptions in cryptography

- 1. Factoring is hard:** given a 400 digit number that is a product of two 200 digit primes, can't efficiently find these primes.
- 2. Discrete logarithm is hard:** given a 300 digit prime and the result of exponentiation mod this prime, find the logarithm, i.e. find  $k$  when given  $a^k \bmod p$ .

# Application 4: key exchange

Rosen Sec 4.6, p. 302

Fix  $a, p$ , sender's private key  $k_1$ , receiver's private key  $k_2$

*Idea: exchange information so that sender and receiver will have shared **key** (number) but no-one looking at messages will be able to decode them without knowing either or both of  $k_1, k_2$*

1. Sender sends  $a^{k_1} \bmod p$  to receiver.
2. Receiver sends  $a^{k_2} \bmod p$  to sender.

Shared key is  $a^{(k_1)(k_2)} \bmod p$

# Diffie & Hellman



# Application 5: Pseudorandom generators

*Rosen p. 288*

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

Parameters:

- modulus  $m$
- multiplier  $a$  ( $2 \leq a < m$ )
- increment  $c$  ( $0 \leq c < m$ )
- seed  $x_0$  ( $0 \leq x_0 < m$ )

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 5: Pseudorandom generators

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

Parameters:

- modulus  $m$
- multiplier  $a$  ( $2 \leq a < m$ )
- increment  $c$  ( $0 \leq c < m$ )
- seed  $x_0$  ( $0 \leq x_0 < m$ )

$m=8, a=5, c=1, x_0=1$

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, ...



# Next up: review for final exam

Final exam is Saturday December 16  
11:30am-2:30pm