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 | (a,s) is in R}

The example

Rosen p. 240

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

iff a mod m = b mod ~~b~~ m ← take remainder

0, . . . , m-1

iff m | (a-b)

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

and in this case, we write $a \equiv b \pmod{m}$

3 | (5-(-1)) ?

$\exists q\,(5-(-1)) = q3$?

Which of the following is true?

m

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.

5 mod 3 : $5 = \boxed{1}\,3 + \boxed{2}$

-1 mod 3 : $-1 = \boxed{-1}\,3 + \boxed{2}$

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

Congruence classes: **$[a]_m$ = {s | (a,s) is in R} = {s | a mod m = s mod m}**

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

E.g. m=6

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

-6
{0, 6, 12, 18, 24, …}
-5
{1, 7, 13, 19, 25, …}
-4
{2, 8, 14, 20, 26, …}

-3
{3, 9, 15, 21, 27, …}
-2
{4, 10, 16, 22, 28, …}
-1
{5, 11, 17, 23, 29, …}

Application 1: Proof by cases

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

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

Proof:

Induction? Structural $\mathbb{Z}$ . . . .

Contradiction? . . - - -

Exhaustive? infinitely many in $\mathbb{Z}$

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.

Alternate strategy: Two cases $<$ n even ... n^2? / n odd ... n^2?

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

Case 0 $\quad n \bmod 4 = 0 \quad$ WTS $n^2 \bmod 4 = 0$ or $n^2 \bmod 4 = 1$

By def, there's int q where $n = 4q + 0 = 4q$

Squaring: $n^2 = 16q^2 = 4\underbrace{(4q^2)}_{\text{int}}$ so $n^2 \bmod 4 = 0$ //

…

Arithmetic modulo *m*

Rosen p. 242-243

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

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

$n^2 \bmod m = ((n \bmod m)(n \bmod m)) \bmod m$

Prev ex: if $n \bmod m = 0$

Arithmetic modulo *m*

Rosen p. 242-243

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

$$\overset{2017\cdot 2017}{ab}\ \mathbf{mod}\ \underset{15}{m} = (\overset{7}{\underbrace{(a\ \mathbf{mod}\ m)}}\ \overset{7}{\underbrace{(b\ \mathbf{mod}\ m)}})\ \mathbf{mod}\ \overset{10}{\underline{m}}$$

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 2: Last digit

$$2017 \times 2017$$

$2017 \bmod 4 = ((\cancel{2000 \bmod 4}) + 17 \bmod 4) \bmod 4 = 1$

What's the last digit of 2017^{2017}?

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

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

$(2017)(2017)(2017) \cdots\cdots (2017)$

$7 \cdot 7 \cdots\cdots 7$

last digits of 7^n: 1, 7, 9, 3, 1, 7, 9, 3, ...

0 1 2 3 0 1 2 3

Modular operations

$a - b = a + (-b)$

$\frac{a}{b} = a \cdot \frac{1}{b}$??

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

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

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

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

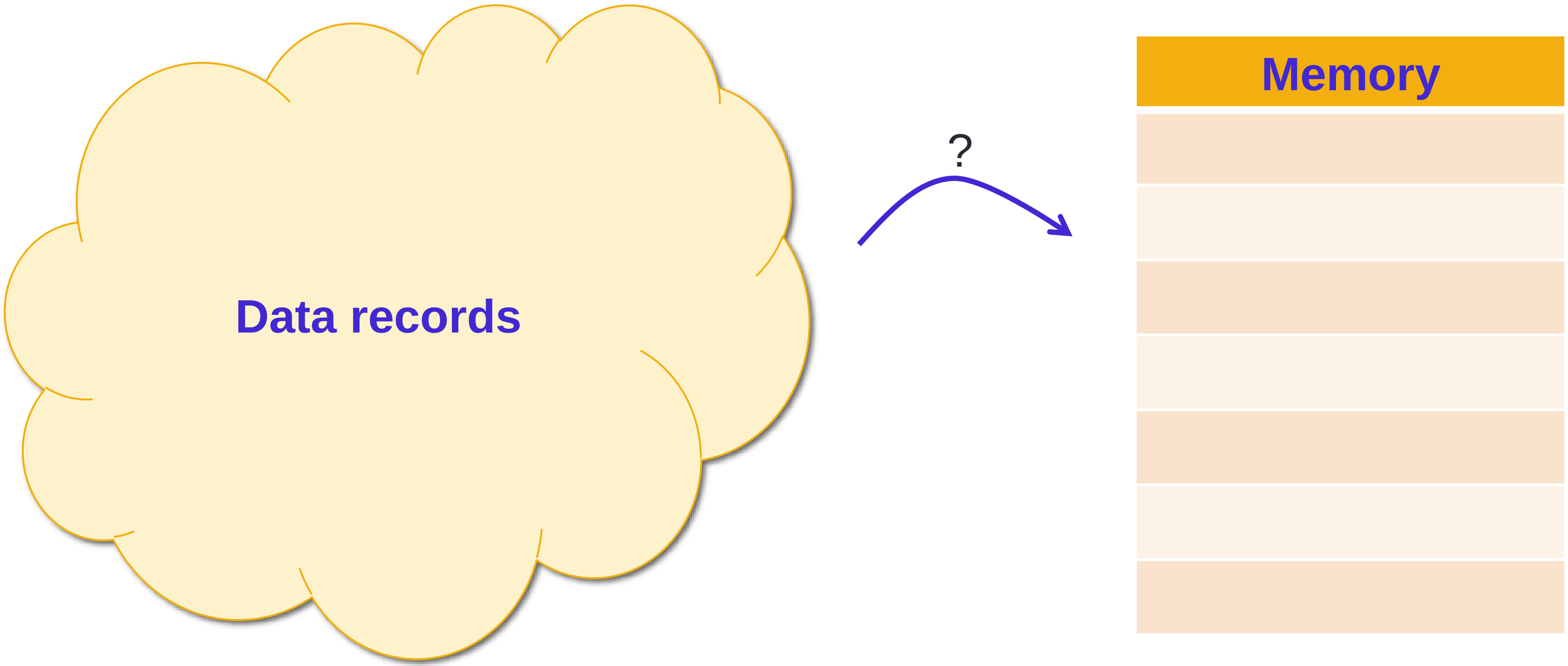
Counterexample: a = 16, b = 8, m = 10

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

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

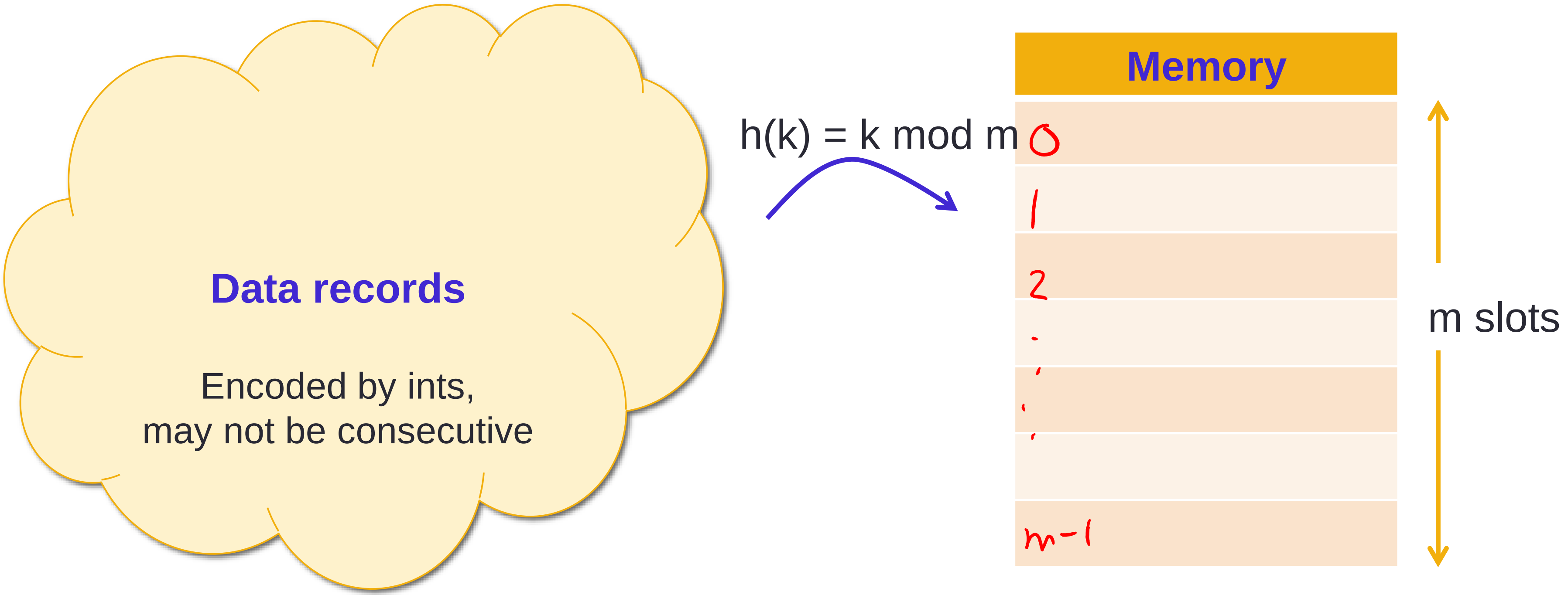
Application 3: hashing

Rosen Sec 4.5 p. 287



Application 3: hashing

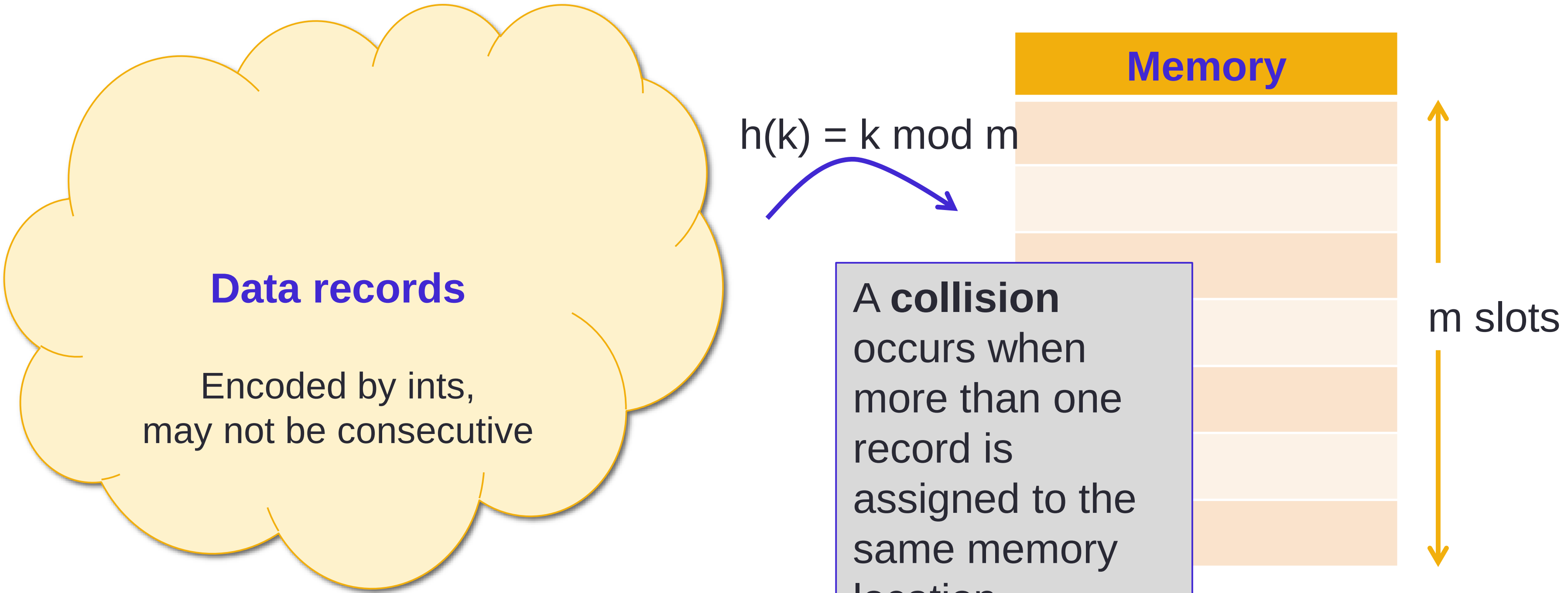
Rosen Sec 4.5 p. 287



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

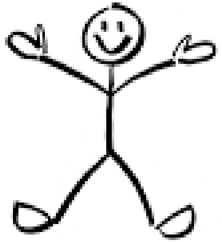
Application 3: hashing

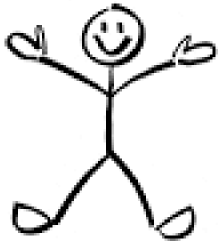
Rosen Sec 4.5 p. 287



A **collision** occurs when more than one record is assigned to the same memory location

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 mod p.

Application 4: key exchange *Rosen Sec 4.6, p. 302*

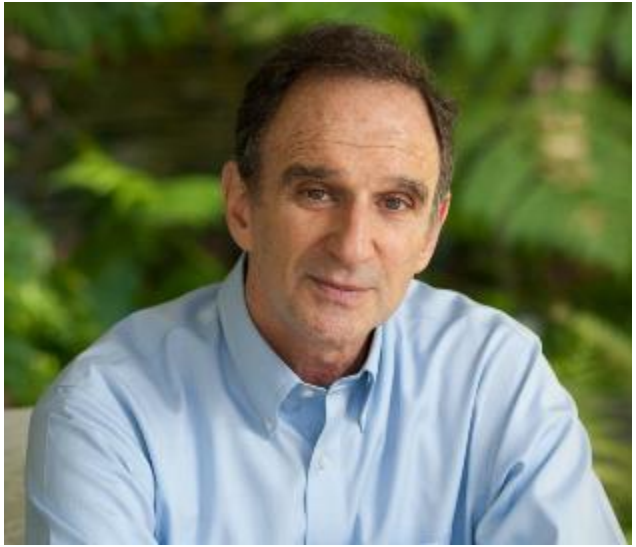
Fix a, p , sender's private key k_1 , receiver's private key k_2

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^{k1} mod p to receiver.
2. Receiver sends a^{k2} mod p to sender.

Shared key is $\mathbf{a^{(k1)(k2)}}$ mod p.

Diffie & Hellman



Application 5: 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 5: Pseudorandom generators

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

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, …

Next up: review for final exam

Final exam is Saturday December 16

11:30am-2:30pm