This week's highlights

- Define (binary) relations and give examples.
- Define equivalence using relations and give examples.
- Use the equivalence relation of congruence modulo integers and apply its properties
- Trace the algorithms involved in Diffie-Helman key exchange
- Trace the algorithms involved in modular exponentiation
- Determine and prove whether a given binary relation is
  - symmetric
  - antisymmetric
  - reflexive
  - transitive
- Determine and prove whether a given binary relation is an equivalence relation
- Determine and prove whether a given binary relation is a partial order
- Draw the Hasse diagram of a partial order

Lecture videos

Week 9 Day 1 YouTube playlist
Week 9 Day 2 YouTube playlist
Week 9 Day 3 YouTube playlist

Monday March 1

Definition: When A and B are sets, we say any subset of $A \times B$ is a **binary relation**. There are other ways to represent a relation R

- A function $f_{TF} : A \times B \to \{T, F\}$ with $f_{TF}(\quad) =$ ____________
- A function $f_{\mathcal{P}} : A \to \mathcal{P}(B)$ with $f_{\mathcal{P}}(\quad) =$ ____________

Definition: When A is a set, we say any subset of $A \times A$ is a (binary) **relation** on A.

Example: For $A = \mathcal{P}(\mathbb{R})$, we can define the relation $EQ_{\mathbb{R}}$ on A as

$$\{(X_1, X_2) \in \mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R}) \mid |X_1| = |X_2|\}$$

Example: Let $R_{(\mathbf{mod}\ n)}$ be the set of all pairs of integers (a, b) such that $(a \ \mathbf{mod}\ n = b \ \mathbf{mod}\ n)$. Then a is **congruent to** b **mod** n means $(a, b) \in R_{(\mathbf{mod}\ n)}$. A common notation is to write this as $a \equiv b (\mathbf{mod}\ n)$.

$R_{(\mathbf{mod}\ n)}$ is a relation on the set ______________________________

Some example elements of $R_{(\mathbf{mod}\ 4)}$ are: ______________________________

Example: Recall that S is defined as the set of all RNA strands, strings made of the bases in $B = \{\mathtt{A}, \mathtt{U}, \mathtt{G}, \mathtt{C}\}$. Define the functions *mutation*, *insertion*, and *deletion* as described by the pseudocode below:

```
procedure mutation(b_1 ··· b_n : a RNA strand , k : a positive integer , b : an element of B)
for i := 1 to n
  if i = k
    c_i := b
  else
    c_i := b_i
return c_1 ··· c_n {The return value is a RNA strand made of the c_i values}
```

```
procedure insertion(b_1 ··· b_n : a RNA strand , k : a positive integer , b : an element of B)
if k > n
  for i := 1 to n
    c_i := b_i
  c_{n+1} := b
else
  for i := 1 to k − 1
    c_i := b_i
  c_k := b
  for i := k + 1 to n + 1
    c_i := b_{i−1}
return c_1 ··· c_{n+1} {The return value is a RNA strand made of the c_i values}
```

```
procedure deletion(b_1 ··· b_n : a RNA strand , k : a positive integer)
if k > n
  m := n
  for i := 1 to n
    c_i := b_i
else
  m := n − 1
  for i := 1 to k − 1
    c_i := b_i
  for i := k to n − 1
    c_i := b_{i+1}
return c_1 ··· c_m {The return value is a RNA strand made of the c_i values}
```

Mut with domain $S \times S$ is defined by, for $s_1 \in S$ and $s_2 \in S$,

$$Mut(s_1, s_2) = \exists k \in \mathbb{Z}^+ \exists b \in B(\ mutation(s_1, k, b) = s_2\ )$$

Ins with domain $S \times S$ is defined by, for $s_1 \in S$ and $s_2 \in S$,

$$Ins(s_1, s_2) = \exists k \in \mathbb{Z}^+ \exists b \in B(\ insertion(s_1, k, b) = s_2\ )$$

Del with domain $S \times S$ is defined by, for $s_1 \in S$ and $s_2 \in S$,

$$Del(s_1, s_2) = \exists k \in \mathbb{Z}^+(\ deletion(s_1, k) = s_2\ )$$

Definition: We say that a RNA strand s_1 is "within one edit" of a RNA strand s_2 to mean

$$Mut(s_1, s_2) \vee Mut(s_2, s_1) \vee Ins(s_1, s_2) \vee Ins(s_2, s_1) \vee Del(s_1, s_2) \vee Del(s_2, s_1)$$

$within1_{TF} : \_\_\_\_\_ \to \_\_\_\_\_$ $\qquad$ $within1_{\mathcal{P}} : \_\_\_\_ \to \_\_\_\_$

$within1_{TF}(s_1, s_2) = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_$ $\qquad$ $within1_{\mathcal{P}}(s_1) = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_$

$W_1 = \{\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\}$

A relation R on a set A is called **reflexive** means $(a, a) \in R$ for every element $a \in A$.

A relation R on a set A is called **symmetric** means $(b, a) \in R$ whenever $(a, b) \in R$, for all $a, b \in A$.

Example: when the domain is $\{a, b, c, d, e, f, g, h\}$ consider the relation $\{(a, b), (b, a), (b, c), (c, b), (f, g), (g, f)\}$.

A relation R on a set A is called **transitive** means whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$, for all $a, b, c \in A$.

Example: when the domain is $\{a, b, c, d, e, f, g, h\}$ consider the relation

$$\{(a, b), (b, a), (b, c), (c, b), (a, a), (b, b), (c, c), (e, g), (f, g), (e, f)\}$$

Relation	Reflexive? (why/why not)	Symmetric? (why/why not)	Transitive? (why/why n
W_1			
$R_{(\mathbf{mod}\ 4)}$			

Wednesday March 3

Definition: (*Rosen 9.1*) A relation R on a set A is called **reflexive** means $(a,a) \in R$ for every element $a \in A$. A relation R on a set A is called **symmetric** means $(b,a) \in R$ whenever $(a,b) \in R$, for all $a,b \in A$. A relation R on a set A is called **transitive** means whenever $(a,b) \in R$ and $(b,c) \in R$, then $(a,c) \in R$, for all $a,b,c \in A$.

Definition: (*Rosen 9.5*) A relation is an **equivalence relation** means it is reflexive, symmetric, and transitive.

Definition: (*Rosen 9.5*) An **equivalence class** of an element $a \in A$ for an equivalence relation R on the set A is the set $\{s \in A | (a,s) \in R\}$. We write this as $[a]_R$.

$$[5]_{R_{(\mathbf{mod}\ 4)}} = \{s \in \mathbb{Z} \mid (5,s) \in R_{(\mathbf{mod}\ 4)}\}$$

Some examples of elements of $[5]_{R_{(\mathbf{mod}\ 4)}}$ are: ____

Some examples of elements of $[9]_{R_{(\mathbf{mod}\ 4)}}$ are: ____

Some examples of elements of $[6]_{R_{(\mathbf{mod}\ 4)}}$ are: ____

Definition: A **partition** of a set A is a set of non-empty, disjoint subsets $A_1, A_2, \cdots, A_n$ such that $A_1 \cup A_2 \cup \cdots \cup A_n = A$.

We can partition the set of integers using equivalence classes of $R_{(\mathbf{mod}\ 4)}$

$$\mathbb{Z} = [0]_{R_{(\mathbf{mod}\ 4)}} \ \cup\ [1]_{R_{(\mathbf{mod}\ 4)}} \ \cup\ [2]_{R_{(\mathbf{mod}\ 4)}} \ \cup\ [3]_{R_{(\mathbf{mod}\ 4)}}$$

Recall: We say a is **congruent to** b **mod** n means $(a,b) \in R_{(\mathbf{mod}\ n)}$. A common notation is to write this as $a \equiv b(\mathbf{mod}\ n)$.

Modular arithmetic:

$(102 + 48)$ **mod** $10 =$ ________________________________

$(7 \cdot 10)$ **mod** $5 =$ ________________________________

(2^5) **mod** $3 =$ ________________________________

Lemma (Section 4.1 Theorem 5): For $a,b \in \mathbb{Z}$ and positive integer n, if $a \equiv b(\mathbf{mod}\ n)$ and $c \equiv d(\mathbf{mod}\ n)$ then $a + c \equiv b + d(\mathbf{mod}\ n)$ and $ac \equiv bd(\mathbf{mod}\ n)$. **Informally**: can bring mod "inside" and do it first, for addition and for multiplication.

Lemma (Section 4.1, page 241): For $a, b \in \mathbb{Z}$ and positive integer n, $(a, b) \in R_{(\mathbf{mod}\ n)}$ if and only if $n | a - b$.

Application: Cycling

How many minutes past the hour are we at? *Model with* $+15$ **mod** 60

Time:	12:00pm	12:15pm	12:30pm	12:45pm	1:00pm	1:15pm	1:30pm	1
"Minutes past":	0	15	30	45	0	15	30	

Replace each English letter by a letter that's fifteen ahead of it in the alphabet *Model with* $+15$ **mod** 26

Original index:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Original letter:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
Shifted letter:	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
Shifted index:	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10

Application: Cryptography

Definition: Let a be a positive integer and p be a large[1] prime number, both known to everyone. Let k_1 be a secret large number known only to person P_1 (Alice) and k_2 be a secret large number known only to person P_2 (Bob). Let the **Diffie-Helman shared key** for a, p, k_1, k_2 be $(a^{k_1 \cdot k_2} \textbf{ mod } p)$.

Idea: P_1 can quickly compute the Diffie-Helman shared key knowing only a, p, k_1 and the result of $a^{k_2} \textbf{ mod } p$ (that is, P_1 can compute the shared key without knowing k_2, only $a^{k_2} \textbf{ mod } p$). Further, any person P_3 who knows neither k_1 nor k_2 (but may know any and all of the other values) cannot compute the shared secret efficiently.

Key Property: $\forall a \in \mathbb{Z}\, \forall b \in \mathbb{Z}\, \forall g \in \mathbb{Z}^+\, \forall n \in \mathbb{Z}^+ ((g^a \textbf{ mod } n)^b, (g^b \textbf{ mod } n)^a) \in R_{(\textbf{mod } n)}$

[1] We leave the definition of "large" vague here, but think hundreds of digits for practical applications. In practice, we also need a particular relationship between a and p to hold, which we leave out here. See more in Rosen, 4.6, p302.

Friday March 5

Modular Exponentation; Algorithm 5 in Section 4.2 (page 254)

```
procedure modular exponentiation(b: integer;
          n = (a_{k-1}a_{k-2}...a_1a_0)_2, m: positive integers)
x := 1
power := b mod m
for i:= 0 to k-1
   if a_i = 1 then x:= (x · power) mod m
   power := (power · power) mod m
return x {x equals b^n mod m}
```

Calculate 3^8 **mod** 7

Approach 1: Directly

3^1 **mod** $7 =$

3^2 **mod** $7 =$

3^3 **mod** $7 =$

3^4 **mod** $7 =$

3^5 **mod** $7 =$

3^6 **mod** $7 =$

3^7 **mod** $7 =$

3^8 **mod** $7 =$

How many multiplication operations did we use?

Approach 2: Using Algorithm 5

$b =$ ____, $n =$ __________, $k =$ ____, $m =$

i	a_i	x	*power*
		1	b **mod** $m =$
0			
1			
2			
3			

How many multiplication operations did

For a binary relation R on a set A:

R is **reflexive** means $\forall a \in A\ (\ (a,a) \in R\ )$

R is **symmetric** means $\forall a \in A\ \forall b \in A\ \ (\ (a,b) \in R \to (b,a) \in R\ )$

R is **transitive** means whenever $\forall a \in A\, \forall b \in A\, \forall c \in A\ (\ (\ (a,b) \in R \land (b,c) \in R\ ) \to (a,c) \in R$

R is **antisymmetric** means $\forall a \in A\, \forall b \in A\ (\ (\ (a,b) \in R \land (b,a) \in R\ ) \to a = b\ )$

New

Example:

$$\{(X_1, X_2) \in \mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R}) \mid |X_1| = |X_2|\}$$

is a reflexive, symmetric, transitive binary relation on $\mathcal{P}(\mathbb{R})$. Is it antisymmetric?

Example: $R_{(\mathbf{mod}\ n)}$ is the set of all pairs of integers (a,b) such that $(a\ \mathbf{mod}\ n = b\ \mathbf{mod}\ n)$ is a reflexive, symmetric, transitive binary relation on $\mathbb{Z}$. Is it antisymmetric?

Example: On the set $\mathcal{P}(\{1,2\})$, define the binary relation $\{(X,Y) \mid X \subseteq Y\}$. Is it reflexive? Is it symmetric? Is it antisymmetric? Is it transitive?

Example: On the set $\mathbb{Z}$, define the binary relation $\{(x,y) \mid x < y\}$. Is it reflexive? Is it symmetric? Is it antisymmetric? Is it transitive?

What's an example of a set and a relation on that set that is reflexive, not symmetric, and transitive?

Definition: (*Rosen 9.6*) A relation is a **partial ordering** (or partial order) means it is reflexive, anitsymmetric, and transitive.

For a partial ordering, its **Hasse diagram** is a graph whose nodes (vertices) are the elements of the domain of the binary relation and which are located such that nodes connected to nodes above them by (undirected) edges indicate that the relation holds between the lower node and the higher node. Moreover, the diagram omits self-loops and omits edges that are guaranteed by transitivity.

Example: On the set $\mathcal{P}(\{1,2\})$, the binary relation $\{(X,Y) \mid X \subseteq Y\}$ is a partial ordering.

Example: On the set $\mathbb{Z}$, define the binary relation $\{(x,y) \mid x \leq y\}$.

Example: On the set $\mathbb{Z}$, define the binary relation $\{(x,y) \mid x \geq y\}$.

Example: On the set $\mathbb{Z}^+$, define the binary relation $\{(x,y) \mid F(x,y)\}$ where $F(x,y)$ means $\exists c \in \mathbb{Z}$ ($y = cx$)

Review quiz questions

1. **Monday** Recall that the relation $EQ_{\mathbb{R}}$ on $\mathcal{P}(\mathbb{R})$ is

$$\{(X_1, X_2) \in \mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R}) \mid |X_1| = |X_2|\}$$

and $R_{(\textbf{mod } n)}$ is the set of all pairs of integers (a, b) such that $(a \textbf{ mod } n = b \textbf{ mod } n)$ and $W_1 = \{(s_1, s_2) \in S \times S \mid s_1, s_2 \text{ are within 1 edit}\}$.

Select all and only the correct items.

(a) $(\mathbb{Z}, \mathbb{R}) \in EQ_{\mathbb{R}}$

(b) $(0, 1) \in EQ_{\mathbb{R}}$

(c) $(\emptyset, \emptyset) \in EQ_{\mathbb{R}}$

(d) $(-1, 1) \in R_{(\textbf{mod } 2)}$

(e) $(1, -1) \in R_{(\textbf{mod } 3)}$

(f) $(4, 16, 0) \in R_{(\textbf{mod } 4)}$

(g) $(\texttt{AAA}, \texttt{AA}) \in W_1$

(h) $(\texttt{AAA}, \texttt{CCC}) \in W_1$

2. **Monday** Recall that in a movie recommendation system, each user's ratings of movies is represented as a n-tuple (with the positive integer n being the number of movies in the database), and each component of the n-tuple is an element of the collection $\{-1, 0, 1\}$.

Assume there are five movies in the database, so that each user's ratings can be represented as a 5-tuple. Consider the following two binary relations on the set of all 5-tuples where each component of the 5-tuple is an element of the collection $\{-1, 0, 1\}$.

$G_1 = \{(u, v) \mid \text{the ratings of users } u \text{ and } v \text{ agree about the first movie in the database}\}$

$G_2 = \{(u, v) \mid \text{the ratings of users } u \text{ and } v \text{ agree about at least two movies}\}$

Binary relations that satisfy certain properties (namely, are reflexive, symmetric, and transitive) can help us group elements in a set into categories.

(a) **True** or **False**: The relation G_1 holds of $u = (1, 1, 1, 1, 1)$ and $v = (-1, -1, -1, -1, -1)$

(b) **True** or **False**: The relation G_2 holds of $u = (1, 0, 1, 0, -1)$ and $v = (-1, 0, 1, -1, -1)$

(c) **True** or **False**: G_1 is reflexive; namely, $\forall u\ (\ (u, u) \in G_1\ )$

(d) **True** or **False**: G_1 is symmetric; namely, $\forall u\ \forall v\ (\ (u, v) \in G_1 \rightarrow (v, u) \in G_1\ )$

(e) **True** or **False**: G_1 is transitive; namely, $\forall u\, \forall v\, \forall w(\ ((u, v) \in G_1 \wedge (v, w) \in G_1) \rightarrow (u, w) \in G_1\ )$

(f) **True** or **False**: G_2 is reflexive; namely, $\forall u\ (\ (u, u) \in G_2\ )$

(g) **True** or **False**: G_2 is symmetric; namely, $\forall u\ \forall v\ (\ (u, v) \in G_2 \rightarrow (v, u) \in G_2\ )$

(h) **True** or **False**: G_2 is transitive; namely, $\forall u\, \forall v\, \forall w(\ ((u, v) \in G_2 \wedge (v, w) \in G_2) \rightarrow (u, w) \in G_2\ )$

3. **Wednesday** Fill in the blanks in the following proof that, for any equivalence relation R on a set A,

$$\forall a \in A \; \forall b \in A \; ((a, b) \in R \leftrightarrow [a]_R \cap [b]_R \neq \emptyset)$$

Proof: Towards a **(a)**________________, consider arbitrary elements a, b in A. We will prove the biconditional statement by proving each direction of the conditional in turn.

Goal 1: we need to show $(a, b) \in R \to [a]_R \cap [b]_R \neq \emptyset$ *Proof of Goal 1*: Assume towards a **(b)**________________ that $(a, b) \in R$. We will work to show that $[a]_R \cap [b]_R \neq \emptyset$. Namely, we need an element that is in both equivalence classes, that is, we need to prove the existential claim $\exists x \in A \; (x \in [a]_R \wedge x \in [b]_R)$. Towards a **(c)**________________, consider $x = b$, an element of A by definition. By **(d)**________________ of R, we know that $(b, b) \in R$ and thus, $b \in [b]_R$. By assumption in this proof, we have that $(a, b) \in R$, and so by definition of equivalence classes, $b \in [a]_R$. Thus, we have proved both conjuncts and this part of the proof is complete.

Goal 2: we need to show $[a]_R \cap [b]_R \neq \emptyset \to (a, b) \in R$ *Proof of Goal 2*: Assume towards a **(e)**________________ that $[a]_R \cap [b]_R \neq \emptyset$. We will work to show that $(a, b) \in R$. By our assumption, the existential claim $\exists x \in A \; (x \in [a]_R \wedge x \in [b]_R)$ is true. Call w a witness; thus, $w \in [a]_R$ and $w \in [b]_R$. By definition of equivalence classes, $w \in [a]_R$ means $(a, w) \in R$ and $w \in [b]_R$ means $(b, w) \in R$. By **(f)**________________ of R, $(w, b) \in R$. By **(g)**________________ of R, since $(a, w) \in R$ and $(w, b) \in R$, we have that $(a, b) \in R$, as required for this part of the proof.

Consider the following expressions as options to fill in the two proofs above. Give your answer as one of the numbers below for each blank a-c. You may use some numbers for more than one blank, but each letter only uses one of the expressions below.

- i exhaustive proof
- ii proof by universal generalization
- iii proof of existential using a witness
- iv proof by cases
- v direct proof
- vi proof by contrapositive

vii proof by contradiction

viii reflexivity

ix symmetry

x transitivity

4. **Friday** Consider the binary relation on $\mathbb{Z}^+$ defined by $\{(a,b) \mid \exists c \in \mathbb{Z}(b = ac)\}$. Select all and only the properties that this binary relation has.

   (a) It is reflexive.

   (b) It is symmetric.

   (c) It is transitive.

   (d) It is antisymmetric.

5. **Friday** Consider the partial order on the set $\mathcal{P}(\{1,2,3\})$ given by the binary relation $\{(X,Y) \mid X \subseteq Y\}$

   (a) How many nodes are in the Hasse diagram of this partial order?

   (b) How many edges are in the Hasse diagram of this partial order?