

# Relations (Chapter 11)

A few slides have been taken from the sites

<http://cse.unl.edu/~choueiry/S13-235/>

and

[http://www.math-cs.gordon.edu/courses/  
mat231/notes.html](http://www.math-cs.gordon.edu/courses/mat231/notes.html)

# Outline

- Relations
- Properties of relations
- Equivalence relations
- Relations between sets
- Partial Orders
- Hasse Diagrams

# Relations

- Suppose  $A = \{1,2,3,4,5,6\}$
- Consider the set  $L = \{ (x,y): x, y \in A \text{ and } x < y \}$

# Relations

- Suppose  $A = \{1,2,3,4,5,6\}$
- Consider the set  $L = \{ (x,y): x, y \in A \text{ and } x < y \}$
- $L = \{(1,2), (1,3), (1,4), (1,5), (1,6), (2,3), (2,4), (2,5), (2,6), (3,4), (3,5), (3,6), (4,5), (4,6), (5,6)\}$

# Relations

- Suppose  $A = \{1,2,3,4,5,6\}$
- Consider the set  $L = \{ (x,y): x, y \in A \text{ and } x < y \}$
- $L = \{(1,2), (1,3), (1,4), (1,5), (1,6), (2,3), (2,4), (2,5), (2,6), (3,4), (3,5), (3,6), (4,5), (4,6), (5,6)\}$
- Consider the set  $D = \{(x,y): x, y \in A \text{ and } x \mid y\}$

# Relations

- Suppose  $A = \{1,2,3,4,5,6\}$
- Consider the set  $L = \{ (x,y): x, y \in A \text{ and } x < y \}$
- $L = \{(1,2), (1,3), (1,4), (1,5), (1,6), (2,3), (2,4), (2,5), (2,6), (3,4), (3,5), (3,6), (4,5), (4,6), (5,6)\}$
- Consider the set  $D = \{(x,y): x, y \in A \text{ and } x \mid y\}$
- $D = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,2), (2,4), (2,6), (3,3), (3,6), (4,4), (5,5), (6,6)\}$

# Relations

- Suppose  $A = \{1,2,3,4,5,6\}$
- Consider the set  $L = \{ (x,y): x, y \in A \text{ and } x < y \}$
- $L = \{(1,2), (1,3), (1,4), (1,5), (1,6), (2,3), (2,4), (2,5), (2,6), (3,4), (3,5), (3,6), (4,5), (4,6), (5,6)\}$
- Consider the set  $D = \{(x,y): x, y \in A \text{ and } x \mid y\}$
- $D = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,2), (2,4), (2,6), (3,3), (3,6), (4,4), (5,5), (6,6)\}$
- The symbol  $<$  is usually used to denote the relationship between the elements of  $L$ .
- Similarly, the symbol  $\mid$  is generally used to denote the relationship between the elements of  $A$ .
- $L, D \subseteq A \times A$ .

# Relation of a set

- **Defn:** A **relation**  $R$  on a set  $A$  is a subset  $R \subseteq A \times A$ .  
We often abbreviate the statement  $(x,y) \in R$  as  $xRy$ .  
The statement  $(x,y) \notin R$  is abbreviated as  $x \not R y$ .



# Relation of a set

- **Defn:** A **relation**  $R$  on a set  $A$  is a subset  $R \subseteq A \times A$ .  
We often abbreviate the statement  $(x,y) \in R$  as  $xRy$ .  
The statement  $(x,y) \notin R$  is abbreviated as  $x \not R y$ .

Suppose  $A = \{1, 2, 3, 4\}$ . The following are all relations on  $A$ :

- $R = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$
- $S = \{(1, 1), (1, 3), (2, 2), (2, 4), (3, 1), (3, 3), (4, 2), (4, 4)\}$
- $T = \{(3, 4)\}$
- $U = \{(1, 4), (2, 3), (2, 1)\}$

since each one is a subset of  $A \times A$ .

- Relation may or may not have meaning associated with them

# Examples of Relations

- We have seen that  $<$  relation on  $A = \{1,2,3,4,5,6\}$  is given by
  - $L = \{(1,2), (1,3), (1,4), (1,5), (1,6), (2,3), (2,4), (2,5), (2,6), (3,4), (3,5), (3,6), (4,5), (4,6), (5,6)\}$
- We have also seen that  $|$  relation on  $A = \{1,2,3,4,5,6\}$  is given by
  - $D = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,2), (2,4), (2,6), (3,3), (3,6), (4,4), (5,5), (6,6)\}$
- $L \cap D = \{(1,2), (1,3), (1,4), (1,5), (1,6), (2,4), (2,6), (3,6)\}$ .
- $L \cap D = \{(x,y) : x, y \in A \text{ and } x < y \text{ and } x|y\}$
- Note that  $L \cap D$  is a relation.

# Relations

- Binary relations  $R$  defined on a set  $A$
- $R \subseteq A \times A : n = 2$
- $R \subseteq \mathbf{R} \times \mathbf{R} : \text{real plane}$
- $R \subseteq \mathbf{R}^+ \times \mathbf{R}^+ : \text{Interior of the first quadrant}$
- $(a,b) \in R$  is an element of  $R$ .
  - In the text infix notation  $aRb$  is also used.

# Relations as Subsets

Question : Suppose we have relations on  $\{1,2\}$  given by  $R = \{(1,1), (2,2)\}$ ,  $S = \{(1,1), (1,2)\}$ . Find:

- The union  $R \cup S$
- The intersection  $R \cap S$
- The symmetric difference  $R \oplus S$
- The difference  $R - S$
- The complement of  $R$

# Relations as Subsets

Answer: ( $R = \{(1,1), (2,2)\}$ ,  $S = \{(1,1), (1,2)\}$ )

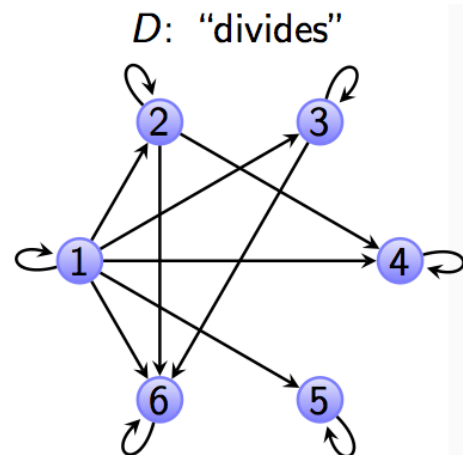
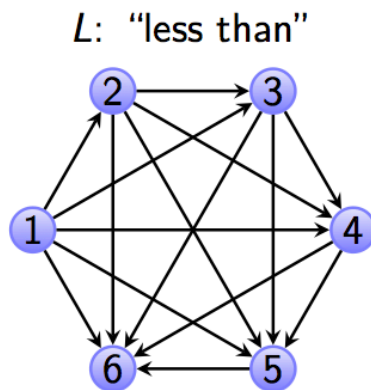
- $R \cup S = \{(1,1), (1,2), (2,2)\}$
- $R \cap S = \{(1,1)\}$
- $R \oplus S = \{(1,2), (2,2)\}$ .
- $R - S = \{(2,2)\}$ .
- $\overline{R} = \{(1,2), (2,1)\}$

# Representing Relations

- There are multiple ways to represent relations.
  1. We have already seen that relations can be enumerated, i.e. they are listed as sets.

# Representing Relations

- There are multiple ways to represent relations.
  - We have already seen that relations can be enumerated, i.e. they are listed as sets.
  - A directed graph can represent a relation  $R$  on  $A$ . Each node (vertex) in the graph represents an element of  $A$  and an arrow from vertex  $x$  to vertex  $y$  indicates  $(x,y) \in R$ . For example, using set  $A$  and relations  $L$  and  $D$  from the previous slides, we have



# Representing Relations

3. A relation  $R$  on  $A = \{a_1, a_2, \dots, a_m\}$  can be represented by the zero-one matrix  $M_R = [m_{ij}]$  with
- $m_{ij} = 1$  if  $(a_i, a_j) \in R$ , and
- $m_{ij} = 0$  if  $(a_i, a_j) \notin R$ .

Note that for creating this matrix we first need to determine the elements that represent the rows. This mapping is arbitrary.



# Representing Relations

Consider the relation  $L$  considered earlier.

$L = \{(1,2), (1,3), (1,4), (1,5), (1,6), (2,3), (2,4), (2,5), (2,6), (3,4), (3,5), (3,6), (4,5), (4,6), (5,6)\}$

$$L = \begin{bmatrix} & .1. & .2. & .3. & .4. & .5. & .6. \\ 1: & 0 & 1 & 1 & 1 & 1 & 1 \\ 2: & 0 & 0 & 1 & 1 & 1 & 1 \\ 3: & 0 & 0 & 0 & 1 & 1 & 1 \\ 4: & 0 & 0 & 0 & 0 & 1 & 1 \\ 5: & 0 & 0 & 0 & 0 & 0 & 1 \\ 6: & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

# Representing Relations

Consider the relation  $D$  considered earlier.

$D = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,2), (2,4), (2,6), (3,3), (3,6), (4,4), (5,5), (6,6)\}$

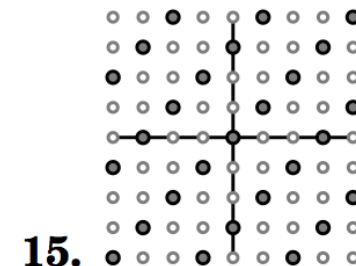
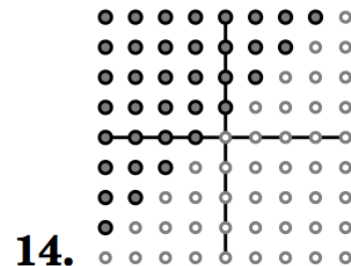
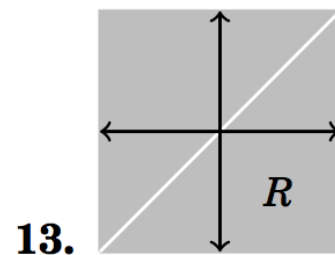
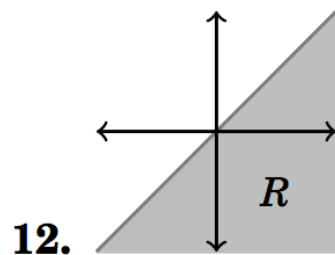
$$D = \begin{bmatrix} & .1. & .2. & .3. & .4. & .5. & .6. \\ 1: & 1 & 1 & 1 & 1 & 1 & 1 \\ 2: & 0 & 1 & 0 & 1 & 0 & 1 \\ 3: & 0 & 0 & 1 & 0 & 0 & 1 \\ 4: & 0 & 0 & 0 & 1 & 0 & 0 \\ 5: & 0 & 0 & 0 & 0 & 1 & 0 \\ 6: & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

# Questions:

- Consider a set  $A$  with  $n$  elements. How many different relations are there on  $A$ ?
- Q.6: Congruence modulo 5 is a relation on set  $\mathbb{N}$  (set of positive integers). Let  $R$  be the relation.
  - $R = \{(a,b) \mid a, b \in \mathbb{N} \text{ and } a \equiv b \pmod{5}\}$
  - $R = \{(0,0), (0,5), (0,10), (1,6), (1,11), \dots\}$

In the following exercises, subsets  $R$  of  $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$  or  $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$  are indicated by gray shading. In each case,  $R$  is a familiar relation on  $\mathbb{R}$  or  $\mathbb{Z}$ . State it.

• Q



# Properties of Binary Relations

- Let  $R$  be a binary relation on  $A$  (i.e.  $R \subseteq A \times A$ )
  - $R$  is **reflexive** if for all  $a \in A$ ,  $(a,a) \in R$ .
  - $R$  is **symmetric** if  $(a,b) \in R$ ,  $(b,a) \in R$ .
  - $R$  is **transitive** if  $(a,b) \in R$ ,  $(b,c) \in R$ , then  $(a,c) \in R$ .
  - $R$  is **antisymmetric** if  $(a,b) \in R$  and  $(b,a) \in R$ ,  $a = b$ .

.

# Properties of Relations in Graphs

- How do each of the properties of relations show up in graphs of relations?
- The graph of a **reflexive** relation will have a loop edge at each node.



# Properties of Relations in Graphs

- How do each of the properties of relations show up in graphs of relations?
- The graph of a **reflexive** relation will have a loop edge at each node.



- The graph of a symmetric relation will not have an edge from x to y unless there is also an edge from y to x.

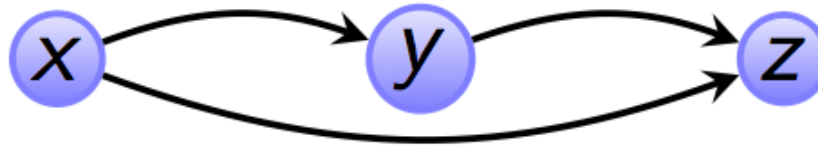


# Properties of Relations in Graphs

- The graph of an **antisymmetric** relation will not have any symmetric pairings. If there is an edge from  $x$  to  $y$ , there cannot be an edge from  $y$  to  $x$ .
- For  $A=\{1,2,3,4,5,6\}$ ,  $R=\{(1,1), (2,2), (3,3), (4,4), (5,5), (6,6)\}$  is a relation which is reflexive, symmetric and antisymmetric.
- A graph is **symmetric** if there is no **antisymmetric** edge. Similarly, a graph is **antisymmetric** if there is no **symmetric** edge.

# Properties of Relations in Graphs

- The graph of a **transitive relation** will have an edge from **x** to **z** whenever there is an edge from **x** to **y** and an edge from **y** to **z**.





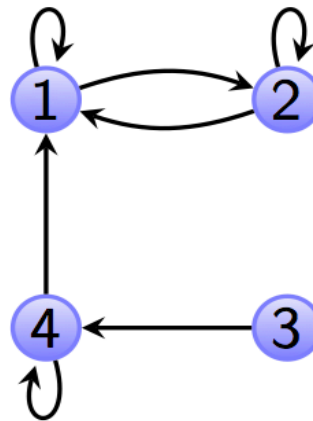
# Examples

Consider the following relations on the set  $\{1, 2, 3, 4\}$ . Determine which ones are reflexive, symmetric, antisymmetric or transitive.

- $R_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$
- $R_2 = \{(1, 1), (1, 2), (2, 1)\}$
- $R_3 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\}$
- $R_4 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$
- $R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$
- $R_6 = \{(3, 4)\}$

$R_1$

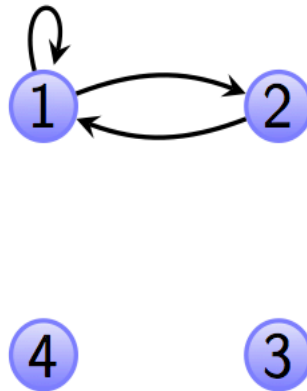
$$R_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$$



- Not reflexive since  $(3, 3)$  is not in  $R_1$  (no loop edge on 3).
- Not symmetric since  $(3, 4) \in R_1$  but  $(4, 3) \notin R_1$ .
- Not antisymmetric since both  $(1, 2)$  and  $(2, 1)$  are in  $R_1$ .
- Not transitive because  $(3, 4)$  and  $(4, 1)$  are both in  $R_1$  but  $(3, 1)$  (a “short-cut” edge) is not.

$R_2$

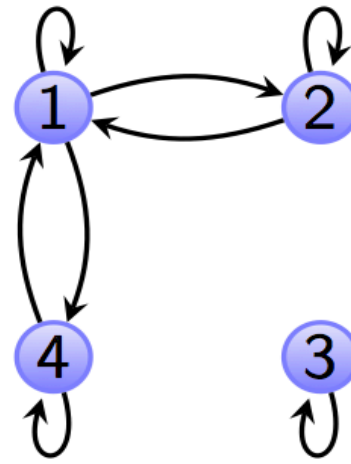
$$R_2 = \{(1, 1), (1, 2), (2, 1)\}$$



- Not reflexive;  $(2, 2) \notin R_2$ .
- Symmetric; there are no non-symmetric connections.
- Not antisymmetric.
- Not transitive because  $(2, 1)$  and  $(1, 2)$  are both in  $R_2$  but  $(2, 2)$  is not.

$R_3$

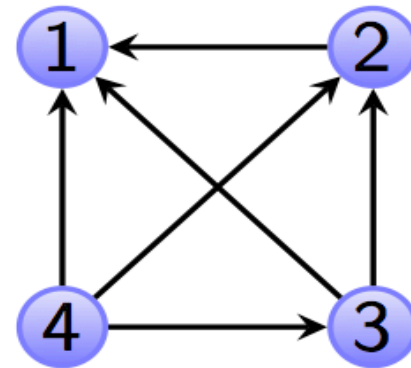
$$R_3 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\}$$



- Reflexive.
- Symmetric.
- Not antisymmetric.
- Not transitive;  $(4, 1), (1, 2) \in R_3$  but  $(4, 2) \notin R_3$ .

$R_4$

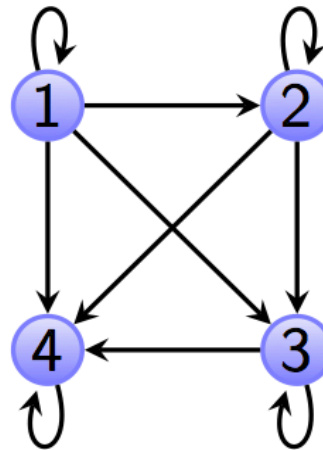
$$R_4 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$$



- Not reflexive.
- Not symmetric.
- Antisymmetric; no symmetric pairs.
- Transitive.

$R_5$

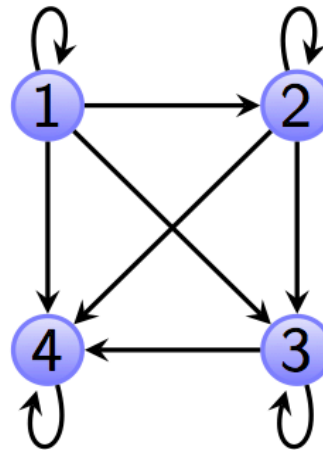
$$R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$$



- Reflexive.
- Not symmetric.
- Antisymmetric; no symmetric pairs.
- Transitive.

$R_5$

$$R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$$

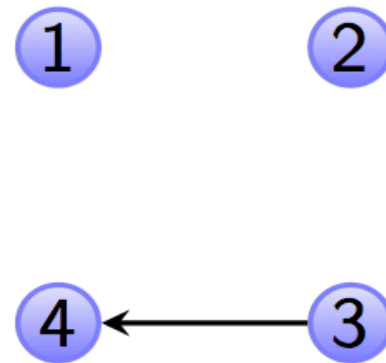


This is the “less than or equal to” relation on  $A=\{1,2,3,4\}$

- Reflexive.
- Not symmetric.
- Antisymmetric; no symmetric pairs.
- Transitive.

$R_6$

$$R_6 = \{(3, 4)\}$$



- Not reflexive.
- Not symmetric.
- Antisymmetric.
- Transitive.



Examine the following table:

Relation on $\mathbb{Z}$	$<$	$\leq$	$=$	$ $	$\nmid$	$\neq$
Reflexive	no	yes	yes	yes	no	no
Symmetric	no	no	yes	no	no	yes
Antisymmetric	yes	yes	yes	yes	no	no
Transitive	yes	yes	yes	yes	no	no

# Visualizing the Properties

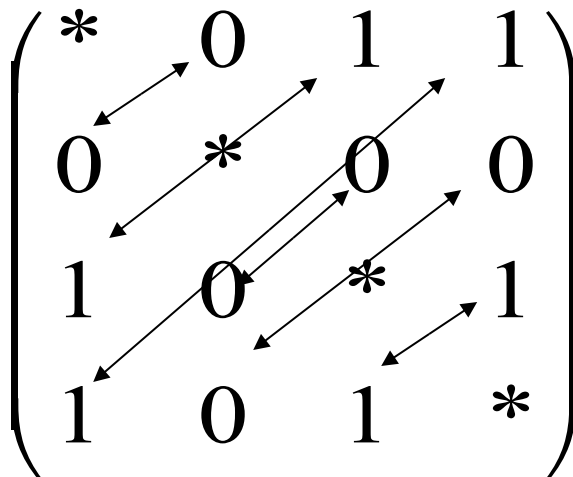
A: Reflexive. Upper-Left corner to Lower-Right corner diagonal is all 1's. EG:

$$M_R = \begin{pmatrix} 1 & * & * & * \\ * & 1 & * & * \\ * & * & 1 & * \\ * & * & * & 1 \end{pmatrix}$$

Q: How about if  $R$  is symmetric?

# Visualizing the Properties

A: A ***symmetric matrix***. i.e., flipping across diagonal does not change matrix. EG:

$$M_R = \begin{pmatrix} * & 0 & 1 & 1 \\ 0 & * & 0 & 0 \\ 1 & 0 & * & 1 \\ 1 & 0 & 1 & * \end{pmatrix}$$


# Visualizing the Properties

- **Not symmetric**

$$M_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

- This matrix is also not **antisymmetric**

## Example 11.8

- **Proposition** Let  $n \in \mathbb{N}$ . The relation  $\equiv (\text{mod } n)$  on the set  $\mathbb{Z}$  is reflexive, symmetric and transitive.  
(It will be proved in the class)

# Counting the number of relations

- Consider set  $A$  where  $|A|=n$ .
- # of relations on  $A$  =
- # of reflexive relations on  $A$  =
- # of symmetric relations of  $A$  =
- # of antisymmetric relations on  $A$  =
- # of transitive relations on  $A$  = hard

# Counting the number of relations

- Consider set  $A$  where  $|A|=n$ .
- # of relations on  $A = 2^{\{n*n\}}$
- # of reflexive relations on  $A = 2^{\{n*n - n\}}$
- # of symmetric relations of  $A = 2^{\{n(n+1)/2\}}$
- # of antisymmetric relations on  $A = 3^{\{n(n-1)/2\}} 2^n$
- # of transitive relations on  $A = \text{hard}$

# Practice problems

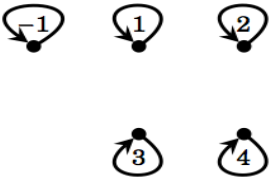
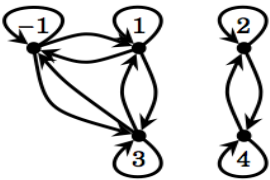
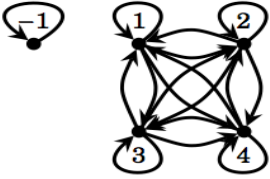
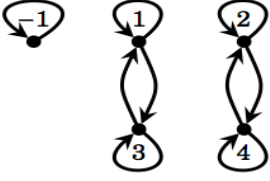
- Section 11.0 : 1, 3, 4, 5, 8
- Section 11.1 : 2, 3, 7, 8, 10, 13, 15



# Equivalence Relation

- Consider the set of every person in the world
- Now consider a  $R$  relation such that  $(a,b) \in R$  if  $a$  and  $b$  are siblings.
- Clearly this relation is
  - Reflexive
  - Symmetric, and
  - Transitive
- Such as relation is called an equivalence relation
- **Definition:** A relation on a set  $A$  is an equivalence relation if it is reflexive, symmetric, and transitive

# Equivalence relation on set $A=\{-1,1,2,3,4\}$

Relation $R$	Diagram	Equivalence classes (see next page)
<p><i>“is equal to”</i> (<math>=</math>)</p> <p><math>R_1 = \{(-1, -1), (1, 1), (2, 2), (3, 3), (4, 4)\}</math></p>		<p><math>\{-1\}, \{1\}, \{2\},</math> <math>\{3\}, \{4\}</math></p>
<p><i>“has same parity as”</i></p> <p><math>R_2 = \{(-1, -1), (1, 1), (2, 2), (3, 3), (4, 4),</math>  <math>(-1, 1), (1, -1), (-1, 3), (3, -1),</math>  <math>(1, 3), (3, 1), (2, 4), (4, 2)\}</math></p>		<p><math>\{-1, 1, 3\}, \{2, 4\}</math></p>
<p><i>“has same sign as”</i></p> <p><math>R_3 = \{(-1, -1), (1, 1), (2, 2), (3, 3), (4, 4),</math>  <math>(1, 2), (2, 1), (1, 3), (3, 1), (1, 4), (4, 1),</math>  <math>(2, 3), (3, 2), (2, 4), (4, 2), (1, 3), (3, 1)\}</math></p>		<p><math>\{-1\}, \{1, 2, 3, 4\}</math></p>
<p><i>“has same parity and sign as”</i></p> <p><math>R_4 = \{(-1, -1), (1, 1), (2, 2), (3, 3), (4, 4),</math>  <math>(1, 3), (3, 1), (2, 4), (4, 2)\}</math></p>		<p><math>\{-1\}, \{1, 3\}, \{2, 4\}</math></p>

**Figure 11.2.** Examples of equivalence relations on the set  $A = \{-1, 1, 2, 3, 4\}$

# Equivalence Relations: Example 1

- **Example:** Let  $R = \{ (a,b) \mid a,b \in \mathbb{R} \text{ and } a \leq b \}$

- Is  $R$  reflexive?
- Is it transitive?
- Is it symmetric?

No, it is not. 4 is related to 5 ( $4 \leq 5$ )  
but 5 is not related to 4

Thus  $R$  is not an equivalence relation

# Equivalence Relations: Example 2

- **Example:** Let  $R = \{ (a,b) \mid a,b \in \mathbb{Z} \text{ and } a=b \}$ 
  - Is  $R$  reflexive?
  - Is it transitive?
  - Is it symmetric?
  - What are the equivalence classes that partition  $\mathbb{Z}$ ?

# Equivalence Relations: Example 3

- **Example:** For  $(x,y),(u,v) \in R^2$ , we define
$$R = \{ ((x,y),(u,v)) \mid (x^2+y^2=u^2+v^2) \}$$
- Show that  $R$  is an equivalence relation.
- What are the equivalence classes that  $R$  defines (i.e., what are the partitions of  $R^2$ )?

# Equivalence Relations: Example 3

- **Example:** For  $(x,y),(u,v) \in \mathbb{R}^2$ , we define

$$R = \{ ((x,y),(u,v)) \mid x^2 + y^2 = u^2 + v^2 \}$$

**Two points are related if they lie on a circle with the center at the origin.**

- Show that  $R$  is an equivalence relation.
- What are the equivalence classes that  $R$  defines (i.e., what are the partitions of  $\mathbb{R}^2$ )?  
**(concentric circles with the center at the origin)**

# Equivalence Class (1)

- **Definition:** Let  $R$  be an equivalence relation on a set  $A$  and let  $a \in A$ . The set of all elements in  $A$  that are related to  $a$  is called the equivalence class of  $a$ . We denote this set  $[a]_R$  or just  $[a]$  if it is clear what  $R$  is.

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

Some examples:

- Suppose  $R = \{(a, b) : a \text{ and } b \text{ were born in the same month}\}$  and is defined on the set of people in this room. Then


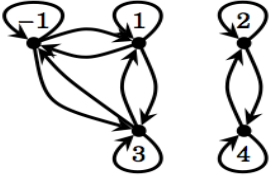
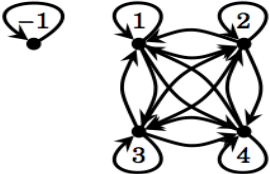
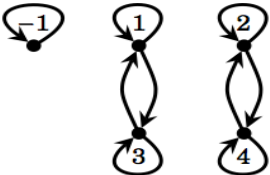
$$[a] = \{b : b \text{ was born in the same month as } a\}.$$

- Suppose  $A = \{1, 2, 3, 4\}$  and  $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (4, 3), (4, 4)\}$ . We can list the equivalence class for each element of  $A$  as

$$[1] = \{1, 2\}, \quad [2] = \{1, 2\}, \quad [3] = \{3, 4\}, \quad [4] = \{3, 4\}$$



# Equivalence relation on set $A=\{-1,1,2,3,4\}$

Relation $R$	Diagram	Equivalence classes (see next page)
<p><i>“is equal to”</i> (<math>=</math>)</p> <p><math>R_1 = \{(-1, -1), (1, 1), (2, 2), (3, 3), (4, 4)\}</math></p>		<p><math>\{-1\}, \{1\}, \{2\},</math> <math>\{3\}, \{4\}</math></p>
<p><i>“has same parity as”</i></p> <p><math>R_2 = \{(-1, -1), (1, 1), (2, 2), (3, 3), (4, 4),</math>  <math>(-1, 1), (1, -1), (-1, 3), (3, -1),</math>  <math>(1, 3), (3, 1), (2, 4), (4, 2)\}</math></p>		<p><math>\{-1, 1, 3\}, \{2, 4\}</math></p>
<p><i>“has same sign as”</i></p> <p><math>R_3 = \{(-1, -1), (1, 1), (2, 2), (3, 3), (4, 4),</math>  <math>(1, 2), (2, 1), (1, 3), (3, 1), (1, 4), (4, 1),</math>  <math>(2, 3), (3, 2), (2, 4), (4, 2), (1, 3), (3, 1)\}</math></p>		<p><math>\{-1\}, \{1, 2, 3, 4\}</math></p>
<p><i>“has same parity and sign as”</i></p> <p><math>R_4 = \{(-1, -1), (1, 1), (2, 2), (3, 3), (4, 4),</math>  <math>(1, 3), (3, 1), (2, 4), (4, 2)\}</math></p>		<p><math>\{-1\}, \{1, 3\}, \{2, 4\}</math></p>

**Figure 11.2.** Examples of equivalence relations on the set  $A = \{-1, 1, 2, 3, 4\}$

# Equivalence Class (2)

- The elements in  $[a]_R$  are called representatives of the equivalence class
- **Theorem:** Let  $R$  be an equivalence class on a set  $A$ . The following statements are equivalent
  1.  $aRb$  (i.e.  $(a,b) \in R$ )
  2.  $[a]=[b]$
  3.  $[a] \cap [b] \neq \emptyset$
- Proof: We first show that  $(1) \Rightarrow (2)$

# Equivalence Class (3)

- We will prove that  $[a] = [b]$  by showing that  $[a] \subseteq [b]$  and  $[b] \subseteq [a]$ .
  - Suppose  $c \in [a]$ .
  - Thus  $(a,c) \in R$ .
  - Because  $(a,b) \in R$ , and  $R$  is symmetric, therefore  $(b,a) \in R$ .
  - Thus  $(b,a) \in R$  and  $(a,c) \in R$ , and  $R$  is transitive, therefore  $(b,c) \in R$ .
  - Because of the symmetric property of  $R$ ,  $(c,b) \in R$  as well.
  - This implies that  $c \in [b]$ .
  - Therefore  $[a] \subseteq [b]$ .
  - The proof for  $[b] \subseteq [a]$  is similar.
  - Hence  $[a] = [b]$ .

# Equivalence Class (4)

- $(2) \Rightarrow (3): [a] = [b] \Rightarrow [a] \cap [b] \neq \emptyset$ 
  - Let  $a, b \in A$  such that  $[a] = [b]$ . Since  $a \in [a]$ , we know that it also belongs to  $[b]$ .
  - This means that  $a \in [a] \cap [b]$ .
  - This implies  $[a] \cap [b] \neq \emptyset$

# Equivalence Class (5)

- $(3) \Rightarrow (1): [a] \cap [b] \neq \emptyset \Rightarrow (a,b) \in R.$ 
  - Let  $c \in [a] \cap [b]$  .  $c$  exists since  $[a] \cap [b]$  is non-empty.
  - Therefore,  $c \in [a]$  and  $c \in [b]$  Since  $a \in [a]$ , we know that it also belongs to  $[b]$ .
  - Thus  $(c,a) \in R$  and  $(c,b) \in R.$
  - $R$  is symmetry:  $(a,c) \in R$  and  $(b,c) \in R.$
  - $R$  is transitive:  $(a,b) \in R.$

# Partitions (1)

- Equivalence classes partition the set  $A$  into disjoint, non-empty subsets  $A_1, A_2, \dots, A_k$
- A **partition** of a set  $A$  satisfies the properties
  - $\bigcup_{i=1}^k A_i = A$
  - $A_i \cap A_j = \emptyset$  for  $i \neq j$
  - $A_i \neq \emptyset$  for all  $i$

# Partitions (2)

- **Example:** Let  $R$  be a relation such that  $(a,b) \in R$  if  $a$  and  $b$  live in the same province/ territories , then  $R$  is an equivalence relation that partitions the set of people who live in Canada into 13 equivalence classes

# Partitions (2)

- **Theorem:**
  - Let  $R$  be an equivalence relation on a set  $S$ . Then the equivalence classes of  $R$  form a partition of  $S$ .
  - Conversely, given a partition  $A_i$  of the set  $S$ , there is a equivalence relation  $R$  that has the set  $A_i$  as its equivalence classes. (**An example is shown in the class.**)



# Partitions: Visual Interpretation

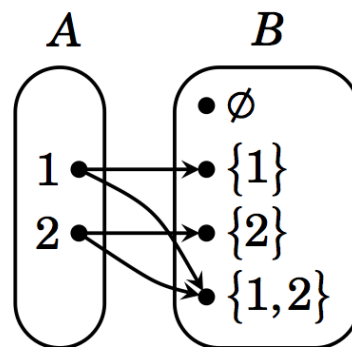
- **Example:** Let  $A=\{1,2,3,4,5,6,7\}$  and  $R$  be an equivalence relation that partitions  $A$  into  $A_1=\{1,2\}$ ,  $A_2=\{3,4,5,6\}$  and  $A_3=\{7\}$ 
  - Draw the 0-1 matrix
  - Draw the digraph
  - (It will be shown in the class.)

# Relations between the sets

- The relations we have seen so far have been relations on a set. We can also define relations between the sets.
- Definition: A real  $R$  from a set  $A$  to set  $B$  is a subset of  $A \times B$ , i.e.  $R \subseteq A \times B$ .

# Relations between the sets

- Example: Suppose  $A = \{1,2\}$  and  $B = \mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$ .
- Let  $R = \{(1, \{1\}), (2, \{2\}), (1, \{1,2\}), (2, \{1,2\})\} \subseteq A \times B$  be a relation from  $A$  to  $B$ .
- The relation  $R$  is the familiar relation  $\in$ .



**Figure 11.3.** A relation from  $A$  to  $B$

# Partial Orders

## (Section 9.6 of Rosen's text)

- Definition: A relation  $R$  on a set  $A$  is a partial order if it is reflexive, antisymmetric and transitive.
- Example: Let  $R$  be a relation on  $\mathbb{N}$  such that  $(a,b) \in R$  if and only if  $a \leq b$ . It can be shown that  $R$  is a partial order.
- We often use the symbol  $\preceq$  for a partial order.

# Posets

- Definition: A set  $A$  together with a partial order relation  $R$  is called a partial ordered set or poset and is denoted by  $(A, R)$ .
- Example: Suppose  $R$  is the relation 'divides'. We can show that  $(\mathbb{N}, R)$  is a poset.

# Comparability and total orders of a poset $(S,R)$

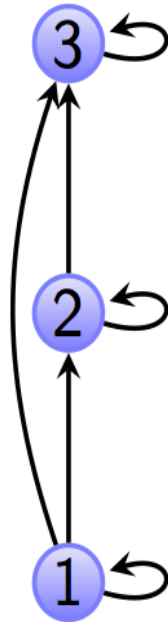
- **Definition:** The elements  $a$  and  $b$  of a poset  $(S,R)$  are called **comparable** if either  $(a,b) \in R$  or  $(b,a) \in R$ .  
Note that both cannot belong to  $R$ . When  $a$  and  $b$  are elements that **neither**  $(a,b) \in R$  nor  $(b,a) \in R$ ,  $a$  and  $b$  are called **incomparable**.
- **Example:** Consider the poset  $(Z,R)$  where  $Z$  is the set of integers and  $R$  indicates the relationship 'divide'.
  - 3 and 6 are comparable
  - 3 and 5 are not comparable.

# Comparability and total orders of a poset $(S,R)$

- **Definition:** If  $(S,R)$  is a poset, and every two elements  $a$  and  $b$  of  $S$  are comparable,  $(S,R)$  is called a **totally ordered set**, and  $R$  is called a total order.
- **Example:**  $(\mathbb{Z}, \leq)$  is a totally ordered set.

# Hasse Diagram to represent posets.

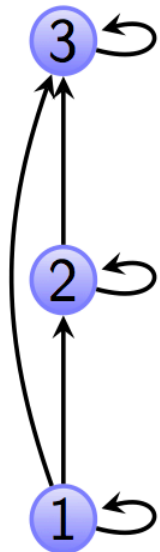
Consider the partial order on  $S = \{1, 2, 3\}$  given by  $(a, b) \in R$  if  $a \leq b$ . We could construct a directed graph of this relation as shown below.



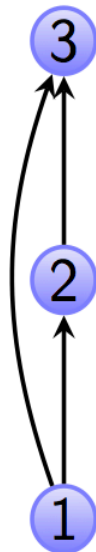


# Hasse Diagram to represent posets.

Original graph



Partial orders are reflexive so we can omit loop edges



Partial orders are transitive so we can omit "short cut" edges

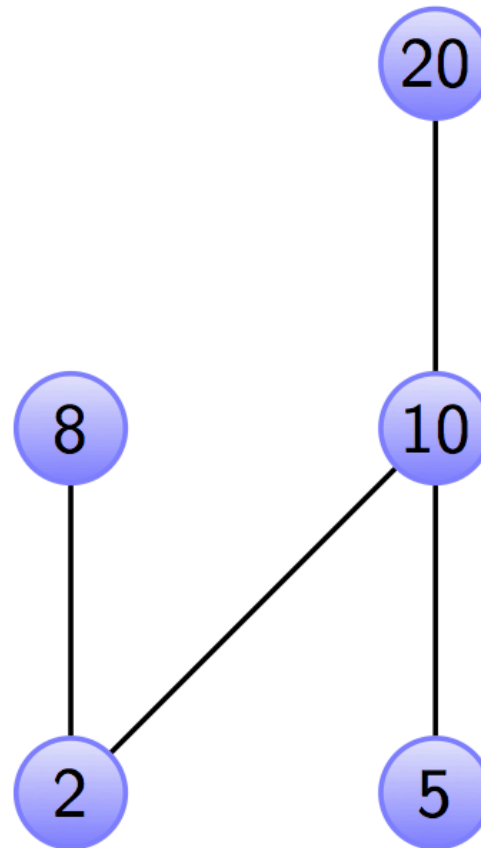


If we always draw arrows up, we can omit arrowheads. This is called a **Hasse Diagram**.



# Hasse Diagram Example

Exercise: Construct the Hasse Diagram for  $(\{2, 5, 8, 10, 20\}, |)$ .

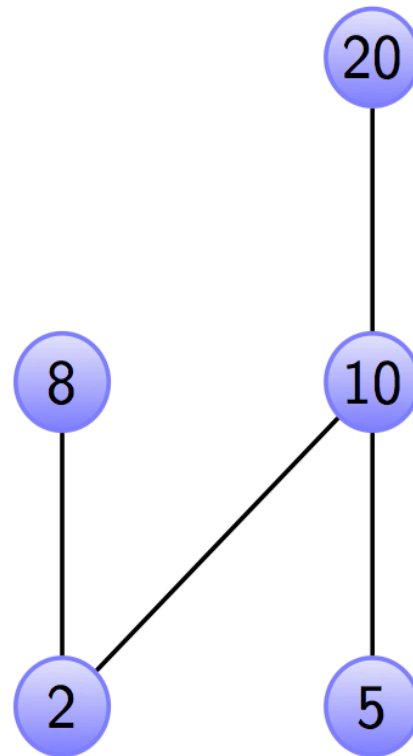


# Hasse Diagram Example

Exercise: Construct the Hasse Diagram for  $(\{2, 5, 8, 10, 20\}, |)$ .

The **maximal elements** of this poset are the “tops;” In this case  $\{8, 20\}$ .

The **minimal elements** are the “bottoms;” in this case  $\{2, 5\}$ .

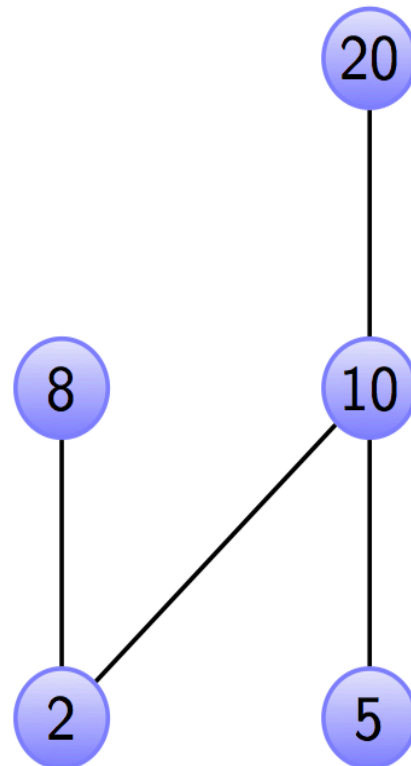


# Hasse Diagram Example

Exercise: Construct the Hasse Diagram for  $(\{2, 5, 8, 10, 20\}, |)$ .

The **maximal elements** of this poset are the “tops;” In this case  $\{8, 20\}$ .

If there is a single maximal element it is the **greatest element**. If there is more than one maximal element then there is no greatest element.



The **minimal elements** are the “bottoms;” in this case  $\{2, 5\}$ .

If there is a single minimal element it is the **least element**. If there is more than one minimal element then there is no least element.

# Practice problems:

- Show that  $(P(A), \subseteq)$  is a poset. Draw the Hasse diagram of  $(P(\{a,b,c\}), \subseteq)$ . Determine the greatest and the least elements of the poset.
- Suppose  $R$  is defined as:  $R = \{(a,b) \mid a, b \in \mathbb{Z} \text{ and } a+b \text{ is even}\}$ .
  - Is  $(\mathbb{Z}, R)$  a poset?
- Consider the 'divides' relation on the set  $A = (1, 2, 2^2, 2^3, \dots, 2^n)$ .
  1. Prove that this relation is a total order on  $A$ .
  2. Draw the Hasse diagram for this relation when  $n=3$ .
- Problems from Rosen Text (9.6): 3, 7, 9, 14, 15, 33 (a), (b), (c), (d), 41.

# Practice problems:

- Section 11.2: 3, 4, 5, 6, 9, 12, 15
- Section 11.3: 2, 3, 4
- Section 11.4: 4, 6, 7, 8

# The Integers modulo $n$

- We have shown that, for  $n \in \mathbb{N}$ ,  $\equiv (\text{mod } n)$  on set  $\mathbb{Z}$  is reflexive, symmetric and transitive, i.e. it is an equivalence relation.
- The equivalence relation  $\equiv (\text{mod } n)$  on  $\mathbb{Z}$  for a given  $n \in \mathbb{N}$  is particularly important in mathematics.
- This relation partitions the integers.
- Consider the case when  $n=5$ .

# The Integers modulo 5

- The equivalence relation  $\equiv (\text{mod } 5)$  partitions  $\mathbb{Z}$  into the following five disjoint sets.

$$[0] = \{x \in \mathbb{Z} : n|(x - 0)\} = \{\dots, -10, -5, 0, 5, 10, 15, \dots\}$$

$$[1] = \{x \in \mathbb{Z} : n|(x - 1)\} = \{\dots, -9, -4, 1, 6, 11, 16, \dots\}$$

$$[2] = \{x \in \mathbb{Z} : n|(x - 2)\} = \{\dots, -8, -3, 2, 7, 12, 17, \dots\}$$

$$[3] = \{x \in \mathbb{Z} : n|(x - 3)\} = \{\dots, -7, -2, 3, 8, 13, 18, \dots\}$$

$$[4] = \{x \in \mathbb{Z} : n|(x - 4)\} = \{\dots, -6, -1, 4, 9, 14, 19, \dots\}$$

- We can define a new set

$$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$$

which we call the integers modulo 5.



# The Integers modulo 5

To get familiar with  $\mathbb{Z}_5$ , let's try a few simple operations.

Consider  $2 \in [2]$  and  $4 \in [4]$ :

- $2 + 4 = 6$  and  $6 \in [1]$ .
- $2 \cdot 4 = 8$  and  $8 \in [3]$ .

Next consider  $7 \in [2]$  and one from  $19 \in [4]$ :

- $7 + 19 = 26$  and  $26 \in [1]$ .
- $7 \cdot 19 = 133$  and  $133 \in [3]$ .

On the one hand, the sum of numbers from  $[2]$  and  $[4]$  was a number from  $[1]$  while on the other hand the product of numbers from  $[2]$  and  $[4]$  was a number from  $[3]$ .

# The Integers modulo 5

Let's try two pairs from another set of equivalence classes, say  $[2]$  and  $[3]$ .

$$2 + 3 = 5 \in [0] \quad \text{and} \quad 2 \cdot 3 = 6 \in [1].$$

Working with different numbers from the same classes we find

$$-3 + 3 = 0 \in [0] \quad \text{and} \quad -3 \cdot 3 = -9 \in [1].$$

Once again, it seems that when we add a number from  $[2]$  to a number from  $[3]$  we obtain a number from  $[0]$ . Similarly, when we multiply a number from  $[2]$  by a number from  $[3]$  we find the product is from  $[1]$ .

# The Integers modulo 5

Just as when you first learned addition and multiplication, it is helpful to construct addition and multiplication tables for  $\mathbb{Z}_5$ .

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

·	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Notice the patterns in each of the tables. In particular, notice that while the order changes, every row and every column contain all five values [0], [1], [2], [3], and [4].

# The Integers modulo 5

- These examples suggest that we can define addition and multiplication for  $Z_5$  as

$$[a] + [b] = [a + b]$$

$$[a].[b]=[a.b]$$

- Note that  $[a]$  and  $[b]$  are sets not numbers.
- Moreover,  $[a] + [b] = [b] + [a]$ , and  $[a].[b] = [b].[a]$ .
- We can also define  $[a] - [b]$ .

# The Integers modulo $n$

- Returning to the general case, we can make the following definition.

**Definition 11.6** Let  $n \in \mathbb{N}$ . The equivalence classes of the equivalence relation  $\equiv (\text{mod } n)$  are  $[0], [1], [2], \dots, [n-1]$ . The **integers modulo  $n$**  is the set  $\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$ . Elements of  $\mathbb{Z}_n$  can be added by the rule  $[a] + [b] = [a + b]$  and multiplied by the rule  $[a] \cdot [b] = [ab]$ .

# Diffie-Hellman Key Exchange

Consider the following problem:

- Two people (or computers) need to communicate securely.
- They have access to a *symmetric cypher* (the same key is used for encryption and decryption).
- They have not yet agreed on a key (they may not have ever met or communicated before).

The challenge here is “how can these two people decide on a key to use without anyone being able to capture it?”

The first effective public key exchange method is known as **Diffie-Hellman Key Exchange** after the researchers that discovered it.

# Diffie-Hellman Key Exchange

Because they were used in the original description of the algorithm, Diffie-Hellman key exchange is usually described assuming that Alice and Bob want to use a symmetric cipher and so need to exchange a private key.

- 1 Alice and Bob agree on two numbers  $g$  and  $p$  with  $0 < g < p$ . These numbers are not private and can be known by anyone.
- 2 Alice picks a private number  $0 < a$  and computes  $\alpha = g^a \bmod p$ . Alice sends  $\alpha$  to Bob.
- 3 Meanwhile, Bob picks a private number  $0 < b$  and computes  $\beta = g^b \bmod p$ . He then sends  $\beta$  to Alice.
- 4 Alice computes  $k = \beta^a \bmod p$  and Bob computes  $k = \alpha^b \bmod p$ . Both of them obtain the same number  $k$  which can then be used as the secret key.

# Diffie-Hellman Key Exchange

Example: Alice and Bob agree on  $g = 327$  and  $p = 919$ .

- Alice chooses  $a = 400$ ; this is her *private key*. She then computes  $\alpha = 327^{400} \bmod 919 = 231$ . This is Alice's *public key* and can be known by anyone. She can send this number to Bob in cleartext.
- Bob chooses  $b = 729$  for his *private key* and computes  $\beta = 327^{729} \bmod 919 = 162$  and sends this number (his *public key*) to Alice.
- Alice computes  $k = 162^{400} \bmod 919 = 206$ .
- Bob computes  $k = 231^{729} \bmod 919 = 206$ .
- $k = 206$  is the secret key that both Alice and Bob will use to encrypt their messages to each other.