Sequences and Series(Sums)

Section Summary

- Sequences.
  - Examples: Geometric Progression, Arithmetic Progression
- Recurrence Relations
  - Example: Fibonacci Sequence
- Summations

Introduction

- Sequences are ordered lists of elements.
- EXAMPLES:
  - 1, 2, 3, 5, 8
  - 1, 3, 9, 27, 81, …….
  - 1, 2, 3, 4, 5, …
  - 4, 8, 12, 16, 20,…
  - 2, 4, 8, 16, 32, …
  - 1, 1/2, 1/3, 1/4, 1/5, …
  - 1, 4, 9, 16, 25, …
  - 1, -1, 1, -1, 1, -1, …
- Sequences arise throughout mathematics, computer science, and in many other disciplines, ranging from botany to music.
- We will introduce the terminology to represent sequences and sums of the terms in the sequences.

SEQUENCES IN COMPUTER PROGRAMMING:

- An important data type in computer programming consists of finite sequences known as one-dimensional arrays; a single variable in which a sequence of variables may be stored.

EXAMPLE:

- The names of k students in a class may be represented by an array of k elements “name” as:

name [0], name[1], name[2], …, name[k-1]

Sequences

Definition: A *sequence* is a function from a subset of the integers (usually either the set {0, 1, 2, 3, 4, ...} or {1, 2, 3, 4, ...}) to a set *S*.

- The notation a_n is used to denote the image of the integer *n*. We can think of a_n as the equivalent of *f(n)* where *f* is a function from {0,1,2,.....} to *S*. We call a_n a *term* of the sequence.

OR

A sequence is just a list of elements usually written in a row.

Sequences

Example: Consider the sequence $\{a_n\}$ where

$$a_n = \frac{1}{n} \qquad \{a_n\} = \{a_1, a_2, a_3, \ldots\}$$

$$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4} \ldots$$

Sequences

EXAMPLE:

Write the first four terms of the sequence defined by the formula: $b_j = 1 + 2^j$, for all integers $j \geq 0$

SOLUTION:

- $b_0 = 1 + 2^0 = 1 + 1 = 2$
- $b_1 = 1 + 2^1 = 1 + 2 = 3$
- $b_2 = 1 + 2^2 = 1 + 4 = 5$
- $b_3 = 1 + 2^3 = 1 + 8 = 9$

REMARK:

The formula $b_j = 1 + 2^j$, for all integers $j \geq 0$ defines an infinite sequence having infinite number of values.

Sequences

- **EXERCISE:**

Compute the first six terms of the sequence defined by the formula

- Cn = 1+ $(-1)^n$ for all integers n ≥ 0

SOLUTION :

- C0 = 1 + $(-1)^0$ = 1 + 1 = 2
- C1 = 1 + $(-1)^1$ = 1 + (-1) = 0
- C2 = 1 + $(-1)^2$ = 1 + 1 = 2
- C3 = 1 + $(-1)^3$ = 1 + (-1) = 0
- C4 = 1 + $(-1)^4$ = 1 + 1 = 2
- C5 = 1 + $(-1)^5$ = 1 + (-1) = 0

REMARK:

1) If n is even, then Cn = 2 and if n is odd, then Cn = 0. Hence, the sequence oscillates endlessly between 2 and 0.

2) An infinite sequence may have only a finite number of

Sequences

EXAMPLE:

Write the first four terms of the sequence defined by

$$C_n = \frac{(-1)^n n}{n+1} \quad \text{for all integers } n \geq 1$$

SOLUTION:

$$C_1 = \frac{(-1)^1(1)}{1+1} = \frac{-1}{2}, C_2 = \frac{(-1)^2(2)}{2+1} = \frac{2}{3}, C_3 = \frac{(-1)^3(3)}{3+1} = \frac{-3}{4}$$

$$And \quad fourth \quad term \; is C_4 = \frac{(-1)^4(4)}{4+1} = \frac{4}{5}$$

REMARK: A sequence whose terms alternate in sign is called an alternating sequence.

Sequences

Find explicit formulas for sequences with the initial terms given:

1) 0, 1, -2, 3, -4, 5, …

SOLUTION:

$a_n = (-1)^{n+1} n$ for all integers $n \geq 0$

2) $1 - \frac{1}{2}, \frac{1}{2} - \frac{1}{3}, \frac{1}{3} - \frac{1}{4}, \frac{1}{4} - \frac{1}{5}, \ldots$

SOLUTION:

$$b_k = \frac{1}{k} - \frac{1}{k+1} \quad \text{for all integers } n \geq 1$$

Sequences

3) 2, 6, 12, 20, 30, 42, 56, ...

SOLUTION:

$$C_n = n(n+1) \text{ for all integers } n \geq 1$$

4) 1/4, 2/9, 3/16, 4/25, 5/36, 6/49, ...

SOLUTION:

$$d_i = \frac{i}{(i+1)^2} \quad \text{for all integers} \quad i \geq 1$$

OR

$$d_j = \frac{j+1}{(j+2)^2} \quad \text{for all integers} \quad j \geq 0$$

Arithmetic Progression OR Sequences

- A sequence in which every term after the first is obtained from the preceding term by adding a constant number is called an arithmetic sequence or arithmetic progression (A.P.)
- The constant number, being the difference of any two consecutive terms is called the common difference of A.P., commonly denoted by “d”.

EXAMPLES:

1. 5, 9, 13, 17, … (common difference = 4)
2. 0, -5, -10, -15, … (common difference = -5)
3. x + a, x + 3a, x + 5a, … (common difference = 2a)

Arithmetic Sequences

GENERAL TERM OF AN ARITHMETIC SEQUENCE:

Let **a** be the first term and **d** be the common difference of an arithmetic sequence. Then the sequence is:

$$a, a+d, a+2d, a+3d, \ldots$$

If a_i, for $i \geq 1$, represents the terms of the sequence then

a_1 = first term = $a = a + (1-1)\,d$

a_2 = second term = $a + d = a + (2-1)\,d$

a_3 = third term = $a + 2d = a + (3-1)\,d$

By symmetry

a_n = nth term = $a + (n-1)d$ for all integers $n \geq 1$.

Arithmetic Sequences

Examples:

1. Let $a = -1$ and $d = 4$:

$$\{s_n\} = \{s_0, s_1, s_2, s_3, s_4, \ldots\} = \{-1, 3, 7, 11, 15, \ldots\}$$

2. Let $a = 7$ and $d = -3$:

$$\{t_n\} = \{t_0, t_1, t_2, t_3, t_4, \ldots\} = \{7, 4, 1, -2, -5, \ldots\}$$

3. Let $a = 1$ and d = 2:

$$\{u_n\} = \{u_0, u_1, u_2, u_3, u_4, \ldots\} = \{1, 3, 5, 7, 9, \ldots\}$$

Arithmetic Sequences

EXAMPLE:

Find the 20th term of the arithmetic sequence

3, 9, 15, 21, …

SOLUTION:

- Here a = first term = 3
- d = common difference = 9 - 3 = 6
- n = term number = 20
- a_{20} = value of 20th term = ?
- Since $a_n = a + (n - 1)\, d;\ n \geq 1$

$\therefore a_{20} = 3 + (20 - 1)\, 6$

$= 3 + 114$

$= 117$

Arithmetic Sequences

EXERCISE:

Find the 36th term of the arithmetic sequence whose 3rd term is 7 and 8th term is 17.

SOLUTION:

Let **a** be the first term and **d** be the common difference of the arithmetic sequence.

Then $a_n = a + (n - 1)d$ $n \geq 1$

$\Rightarrow a_3 = a + (3 - 1)\,d$ and $a_8 = a + (8 - 1)\,d$

Given that $a_3 = 7$ and $a_8 = 17$. Therefore

$7 = a + 2d$……(1) and $17 = a + 7d$……..(2)

Subtracting (1) from (2), we get,

$10 = 5d \Rightarrow d = 2$

Substituting d = 2 in (1) we have

$7 = a + 2(2)$ which gives $a = 3$

Arithmetic Sequences

Thus, $a_n = a + (n - 1)\, d$

$a_n = 3 + (n - 1)\, 2$ (using values of a and d)

Hence the value of 36th term is

$$a_{36} = 3 + (36 - 1)\, 2$$

$$= 3 + 70$$

$$a_{36} = 73$$

Geometric Progression OR Sequence

- A sequence in which every term after the first is obtained from the preceding term by multiplying it with a constant number is called a geometric sequence or geometric progression (G.P.)
- The constant number, being the ratio of any two consecutive terms is called the common ratio of the G.P. commonly denoted by “r”.
- **EXAMPLE:**

1. 1, 2, 4, 8, 16, … (common ratio = 2)

2. 3, - 3/2, 3/4, - 3/8, … (common ratio = - 1/2)

3. 0.1, 0.01, 0.001, 0.0001, … (common ratio = 0.1 = 1/10)

GENERAL TERM OF A GEOMETRIC SEQUENCE:

Let **a** be the first tem and **r** be the common ratio of a geometric sequence. Then the sequence is $a, ar, ar^2, ar^3, \ldots$

If a_i, for $i \geq 1$ represent the terms of the sequence, then

a_1 = first term = $a = ar^{1-1}$

a_2 = second term = $ar = ar^{2-1}$

a_3 = third term = $ar^2 = ar^{3-1}$

.....

.....

a_n = nth term = ar^{n-1}; for all integers $n \geq 1$

Geometric Progression

Examples:

1. Let $a = 1$ and $r = -1$. Then:

$$\{b_n\} = \{b_0, b_1, b_2, b_3, b_4, \ldots\} = \{1, -1, 1, -1, 1, \ldots\}$$

2. Let $a = 2$ and $r = 5$. Then:

$$\{c_n\} = \{c_0, c_1, c_2, c_3, c_4, \ldots\} = \{2, 10, 50, 250, 1250, \ldots\}$$

3. Let $a = 6$ and $r = 1/3$. Then:

$$\{d_n\} = \{d_0, d_1, d_2, d_3, d_4, \ldots\} = \{6, 2, \frac{2}{3}, \frac{2}{9}, \frac{2}{27}, \ldots\}$$

Geometric Sequence

EXAMPLE:

Find the 8th term of the following geometric sequence

$$4, 12, 36, 108, \ldots$$

SOLUTION:

Here a = first term = 4

r = common ratio = $\frac{12}{4} = 3$

n = term number = 8

a_8 = value of 8th term = ?

Since $a_n = ar^{n-1}; \quad n \geq 1$

$\Rightarrow \quad a_8 = (4)(3)^{8-1}$

$= 4\,(2187)$

$= 8748$

Geometric Sequence

EXERCISE:

Write the geometric sequence with positive terms whose second term is 9 and fourth term is 1.

SOLUTION:

Let **a** be the first term and **r** be the common ratio of the geometric sequence. Then

$a_n = ar^{n-1}$ $\quad n \geq 1$

Now $a_2 = ar^{2-1}$

$\Rightarrow \quad 9 = ar$ .....(1)

Also $a_4 = ar^{4-1}$

$1 = ar^3$ .....(2)

Dividing (2) by (1), we get,

$$\frac{1}{9} = \frac{ar^3}{ar}$$

$$\Rightarrow \quad \frac{1}{9} = r^2$$

$$\Rightarrow \quad r = \frac{1}{3} \qquad \left(\text{rejecting } r = -\frac{1}{3}\right)$$

Substituting r = 1/3 in (1), we get

$$9 = a\left(\frac{1}{3}\right)$$

$$\Rightarrow \quad a = 9 \times 3 = 27$$

Hence the geometric sequence is

27, 9, 3, 1, 1/3, 1/9, …

Useful Sequences

TABLE 1 **Some Useful Sequences.**

nth Term	*First 10 Terms*
n^2	1, 4, 9, 16, 25, 36, 49, 64, 81, 100, . . .
n^3	1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, . . .
n^4	1, 16, 81, 256, 625, 1296, 2401, 4096, 6561, 10000, . . .
2^n	2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, . . .
3^n	3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049, . . .
$n!$	1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800, . . .
f_n	1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, . . .

SERIES

The sum of the terms of a sequence forms a series. If $a_1, a_2, a_3, \ldots$ represent a sequence of numbers, then the corresponding series is

$$a_1 + a_2 + a_3 + \ldots = \sum_{k=1}^{\infty} a_k$$

SUMMATIONS

SUMMATION NOTATION:

The capital Greek letter sigma $\sum$ is used to write a sum in a short hand notation.

where k varies from 1 to n represents the sum given in expanded form by

$= a_1 + a_2 + a_3 + \ldots + a_n$

More generally if m and n are integers and $m \leq n$, then the summation from k equal m to n of a_k is

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + a_{m+2} + \cdots + a_n$$

Here **k** is called the index of the summation; **m** the lower limit of the summation and **n** the upper limit of the summation.

SUMMATIONS

COMPUTING SUMMATIONS:

Let $a_0 = 2$, $a_1 = 3$, $a_2 = -2$, $a_3 = 1$ and $a_4 = 0$. Compute each of the summations:

(a) $\sum_{i=0}^{4} a_i$ (b) $\sum_{j=0}^{2} a_{2j}$ (c) $\sum_{k=1}^{1} a_k$

SOLUTION:

(a) $\sum_{i=0}^{4} a_i = a_0 + a_1 + a_2 + a_3 + a_4$
$= 2 + 3 + (-2) + 1 + 0 = 4$

(b) $\sum_{j=0}^{2} a_{2j} = a_0 + a_2 + a_4$
$= 2 + (-2) + 0 = 0$

(c) $\sum_{k=1}^{1} a_k = a_1$
$= 3$

ARITHMETIC SERIES:

The sum of the terms of an arithmetic sequence forms an arithmetic series (A.S). For example

$$1 + 3 + 5 + 7 + \ldots$$

is an arithmetic series of positive odd integers.

In general, if a is the first term and d the common difference of an arithmetic series, then the series is given as: $a + (a+d) + (a+2d) + \ldots$

SUM OF n TERMS OF AN ARITHMETIC SERIES:

Let a be the first term and d be the common difference of an arithmetic series. Then its nth term is:

$$a_n = a + (n - 1)d; \quad n \geq 1$$

If S_n denotes the sum of first n terms of the A.S, then

$$\begin{aligned} S_n &= a + (a + d) + (a + 2d) + \ldots + [a + (n-1)\, d] \\ &= a + (a+d) + (a + 2d) + \ldots + a_n \\ &= a + (a+d) + (a + 2d) + \ldots + (a_n - d) + a_n \quad \ldots\ldots\ldots(1) \end{aligned}$$

where $a_n = a + (n - 1)\, d$

Rewriting the terms in the series in reverse order,

$$S_n = a_n + (a_n - d) + (a_n - 2d) + \ldots + (a + d) + a \quad \ldots\ldots\ldots(2)$$

Adding (1) and (2) term by term, gives

$$2\, S_n = (a + a_n) + (a + a_n) + (a + a_n) + \ldots + (a + a_n) \qquad \text{(n terms)}$$

$$2\, S_n = n\,(a + a_n)$$

$$\Rightarrow \quad S_n = n(a + a_n)/2$$

$$S_n = n(a + l)/2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

Where $l = a_n = a + (n - 1)d$

Therefore

$$S_n = n/2\, [a + a + (n - 1)\, d]$$

$$S_n\ n/2\, [2\, a + (n - 1)\, d] \ldots\ldots\ldots(4)$$

ARITHMETIC SERIES:

EXERCISE:

Find the sum of first n natural numbers.

SOLUTION:

Let $S_n = 1 + 2 + 3 + \ldots + n$

Clearly the right hand side forms an arithmetic series with

$a = 1, \quad d = 2 - 1 = 1 \quad$ and $\quad n = n$

$$\therefore \quad S_n = \frac{n}{2}[2a + (n-1)d]$$

$$= \frac{n}{2}[2(1) + (n-1)(1)]$$

$$= \frac{n}{2}[2 + n - 1]$$

$$= \frac{n(n+1)}{2}$$

GEOMETRIC SERIES:

The sum of the terms of a geometric sequence forms a geometric series (G.S.). For example

$$1 + 2 + 4 + 8 + 16 + \ldots$$

is geometric series.

In general, if **a** is the first term and **r** the common ratio of a geometric series, then the series is given as: $a + ar + ar^2 + ar^3 + \ldots$

Strings

Definition: A *string* is a finite sequence of characters from a finite set (an alphabet).

- Sequences of characters or bits are important in computer science.
- The *empty string* is represented by λ.
- The string *abcde* has *length* 5.

Recurrence Relations

Definition: A *recurrence relation* for the sequence $\{a_n\}$ is an equation that expresses a_n in terms of one or more of the previous terms of the sequence, namely, $a_0, a_1, \ldots, a_{n-1}$, for all integers n with $n \geq n_0$, where n_0 is a nonnegative integer.

- A sequence is called a *solution* of a recurrence relation if its terms satisfy the recurrence relation.
- The *initial conditions* for a sequence specify the terms that precede the first term where the recurrence relation takes effect.

Questions about Recurrence Relations

Example 1: Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1} + 3$ for $n = 1,2,3,4,....$ and suppose that $a_0 = 2$. What are a_1, a_2 and a_3?

[Here $a_o = 2$ is the initial condition.]

Solution: We see from the recurrence relation that

$a_1 = a_o + 3 = 2 + 3 = 5$

$a_2 = 5 + 3 = 8$

$a_3 = 8 + 3 = 11$

Questions about Recurrence Relations

Example 2: Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1} - a_{n-2}$ for $n = 2,3,4,\ldots$ and suppose that $a_0 = 3$ and $a_1 = 5$. What are a_2 and a_3?

[Here the initial conditions are $a_o = 3$ and $a_1 = 5$.]

Solution: We see from the recurrence relation that

$a_2 = a_1 - a_o = 5 - 3 = 2$

$a_3 = a_2 - a_1 = 2 - 5 = -3$

Solving Recurrence Relations

- Finding a formula for the *n*th term of the sequence generated by a recurrence relation is called *solving the recurrence relation*.
- Such a formula is called a *closed formula*.
- Various methods for solving recurrence relations will be covered in Chapter 8 where recurrence relations will be studied in greater depth.
- Here we illustrate by example the method of iteration in which we need to guess the formula. The guess can be proved correct by the method of induction (Chapter 5).

Fibonacci Sequence

Definition: Define the *Fibonacci sequence*, $f_0, f_1, f_2, \ldots$, by:

- Initial Conditions: $f_0 = 0, f_1 = 1$
- Recurrence Relation: $f_n = f_{n-1} + f_{n-2}$

Example: Find f_2, f_3, f_4, f_5 and f_6 .

Answer:

$$f_2 = f_1 + f_0 = 1 + 0 = 1,$$
$$f_3 = f_2 + f_1 = 1 + 1 = 2,$$
$$f_4 = f_3 + f_2 = 2 + 1 = 3,$$
$$f_5 = f_4 + f_3 = 3 + 2 = 5,$$
$$f_6 = f_5 + f_4 = 5 + 3 = 8.$$

Iterative Solution Example

Method 1: Working upward, forward substitution

Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1} + 3$ for $n = 2,3,4,\ldots$ and suppose that $a_1 = 2$.

$$a_2 = 2 + 3$$

$$a_3 = (2 + 3) + 3 = 2 + 3 \cdot 2$$

$$a_4 = (2 + 2 \cdot 3) + 3 = 2 + 3 \cdot 3$$

.

.

.

$$a_n = a_{n-1} + 3 = (2 + 3 \cdot (n - 2)) + 3 = 2 + 3(n - 1)$$

Iterative Solution Example

Method 2: Working downward, backward substitution

Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1} + 3$ for $n = 2,3,4,\ldots.$ and suppose that $a_1 = 2$.

$$a_n = a_{n-1} + 3$$
$$= (a_{n-2} + 3) + 3 = a_{n-2} + 3 \cdot 2$$
$$= (a_{n-3} + 3) + 3 \cdot 2 = a_{n-3} + 3 \cdot 3$$
$$\vdots$$
$$= a_2 + 3(n-2) = (a_1 + 3) + 3(n-2) = 2 + 3(n-1)$$

Some Useful Summation Formulae

TABLE 2 Some Useful Summation Formulae.

Sum	*Closed Form*
$\sum_{k=0}^{n} ar^k \ (r \neq 0)$	$\frac{ar^{n+1} - a}{r - 1}, r \neq 1$
$\sum_{k=1}^{n} k$	$\frac{n(n+1)}{2}$
$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum_{k=0}^{\infty} x^k, \lvert x \rvert < 1$	$\frac{1}{1-x}$
$\sum_{k=1}^{\infty} kx^{k-1}, \lvert x \rvert < 1$	$\frac{1}{(1-x)^2}$

Geometric Series: We just proved this.

Later we will prove some of these by induction.

Proof in text (requires calculus)

Relations

Chapter 9

Mr. SHOAIB RAZA

Chapter Summary

- Relations and Their Properties
- Representing Relations
- Equivalence Relations
- Partial Orderings

Relations and Their Properties

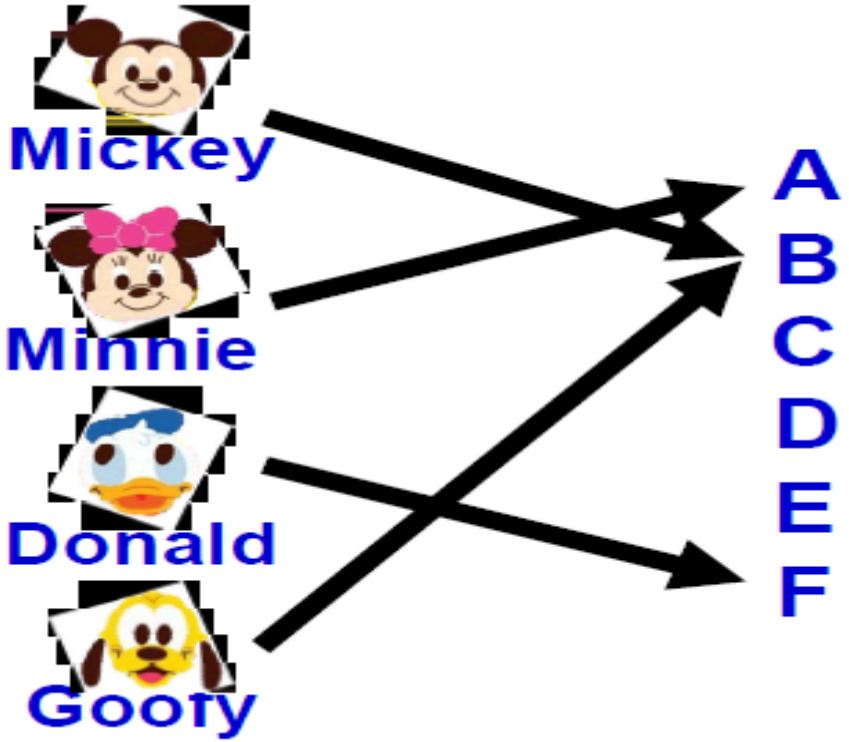
Section 9.1

Section Summary

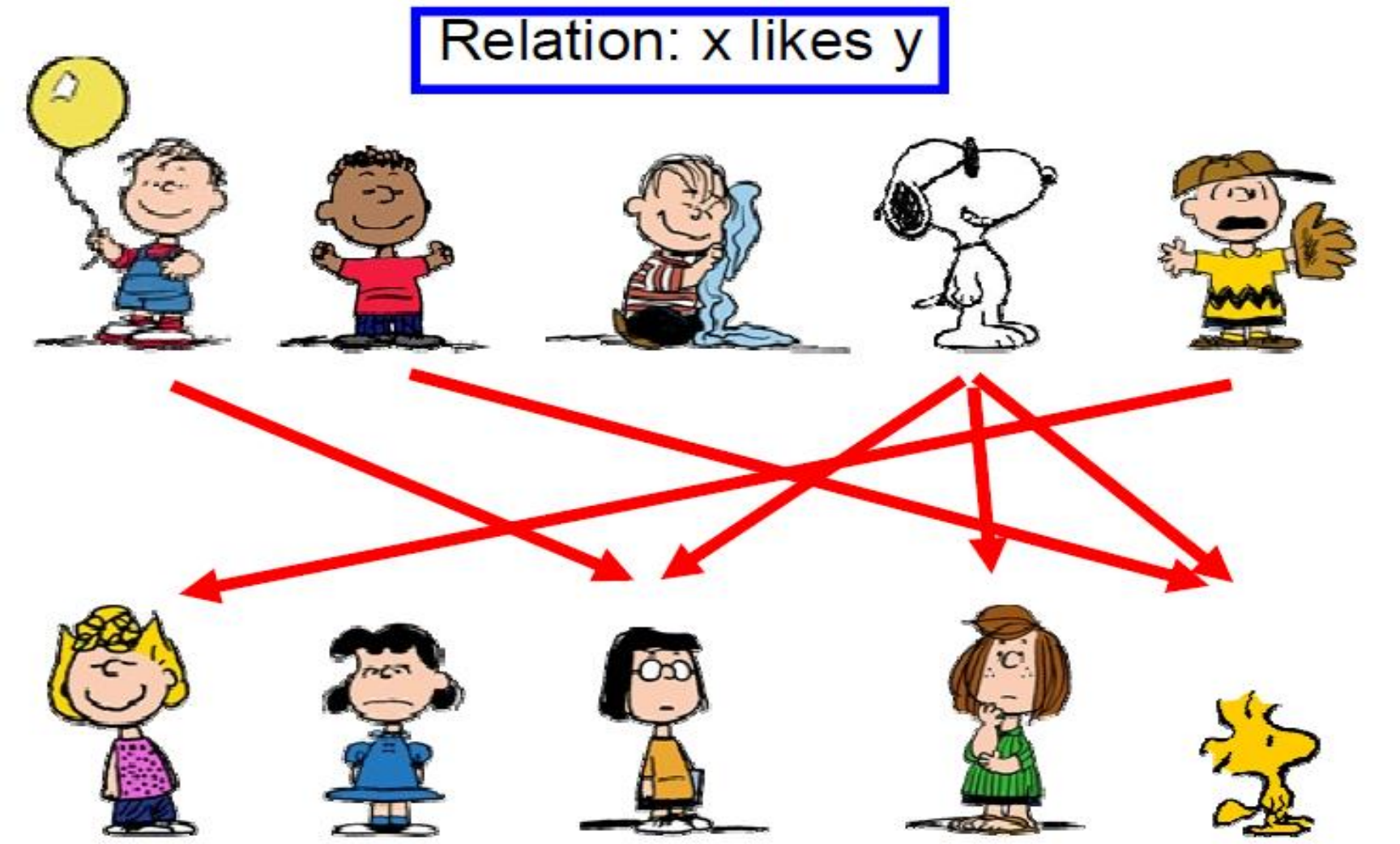
- Relations and Functions
- Properties of Relations
  - Reflexive Relations
  - Symmetric Relations
  - Antisymmetric Relations
  - Transitive Relations
  - Irreflexive Relations
  - Asymmetric Relations
- Combining Relations

Recall, Function is…

- Let **A** and **B** be nonempty sets Function ***f*** from **A** to **B** is an assignment of exactly one element of **B** to each element of **A.**
- By **defining** using a **relation**, a **function** from A to B contains **unique** ordered pair (a, b) for **every** element a ∈ A.



What is Relation?



Binary Relations

Definition: A *binary relation R* from a set *A* to a set *B* is a subset $R \subseteq A \times B$.

- Recall, for example:

  A = {a1, a2} and B = {b1, b2, b3}

  A x B = { (a1, b1), (a1, b2), (a1, b3),
  (a2, b1), (a2, b2), (a2, b3)}

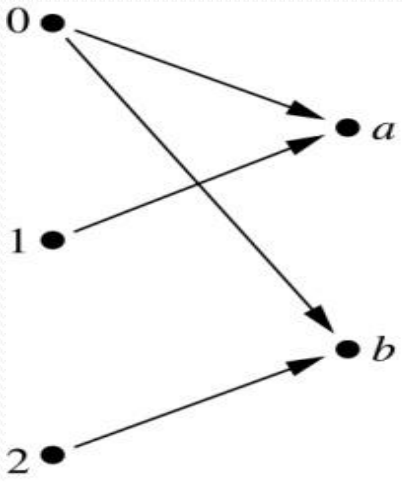
- Ordered pairs, which
  - First element comes from A
  - Second element comes from B
  - **aRb**: (a, b) ∈ R
  - **aRb** : (a, b) ∉ R

Moreover, when (a, b) belongs to R, a is said to be related to b by R.

Binary Relations

Example:

- Let $A = \{0,1,2\}$ and $B = \{a,b\}$
- $\{(0, a), (0, b), (1,a) , (2, b)\}$ is a relation from A to B.
- We can represent relations from a set A to a set B graphically or using a table:



R	a	b
0	×	×
1	×	
2		×

Binary Relations

EXAMPLE:

- Let A = {eggs, milk, corn} and B = {cows, goats, hens}

Define a relation R from A to B by (a, b) ∈R *iff* a is produced by b.

- Then R = {(eggs, hens), (milk, cows), (milk, goats)}
- Thus, with respect to this relation eggs R hens , milk R cows, etc.

Binary Relations

EXAMPLE #1:

- S = {Peter, Paul, Mary}
- C = {C++, DisMath}

- Given
  - Peter takes C++ — Peter R C++ — Peter $\not R$ DisMath
  - Paul takes DisMath — Paul $\not R$ C++ — Paul R DisMath
  - Mary takes none of them — Mary $\not R$ C++ — Mary $\not R$ DisMath

- R = {(Peter, C++), (Paul, DisMath)}

Domain and Range of a Relation

DOMAIN OF A RELATION:

The domain of a relation R from A to B is the set of all first elements of the ordered pairs which belong to R denoted by Dom(R).

Symbolically, $Dom(R) = \{a \in A \mid (a, b) \in R\}$

RANGE OF A RELATION:

The range of a relation R from A to B is the set of all second elements of the ordered pairs which belong to R denoted Ran(R).

Symbolically, $Ran(R) = \{b \in B \mid (a, b) \in R\}$

Domain and Range of a Relation

EXERCISE:

Let A = {1, 2}, B = {1, 2, 3},

Define a binary relation R from A to B as follows:

$R = \{(a, b) \in A \times B \mid a < b\}$ Then

- a. Find the ordered pairs in R.
- b. Find the Domain and Range of R.
- c. Is 1R3, 2R2?

SOLUTION:

Given A = {1, 2}, B = {1, 2, 3},

$A \times B = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)\}$

- a. $R = \{(a, b) \in A \times B \mid a < b\}$

  $R = \{(1,2), (1,3), (2,3)\}$

Domain and Range of a Relation

Given A = {1, 2}, B = {1, 2, 3},

$$A \times B = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)\}$$

- b. Find the Domain and Range of R.

Solution:

Dom(R) = {1,2} and Ran(R) = {2, 3}

- c. Is 1R3, 2R2?

Solution:

c. Since $(1, 3) \in R$ so 1R3.

Since $(2, 2) \in R$ so 2R2.

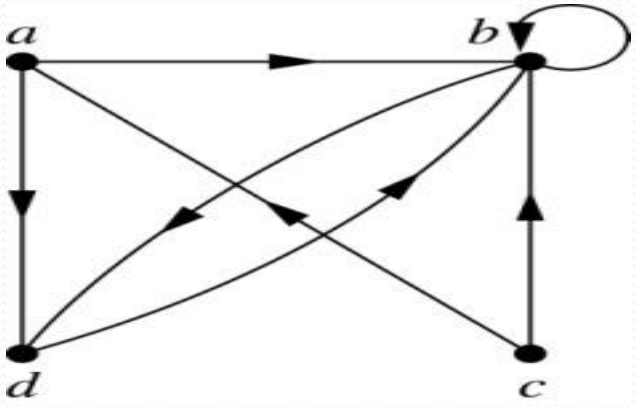
Representing Relations

Representing Relations Using Digraphs

Definition: A *directed graph*, or *digraph*, consists of a set V of *vertices* (or *nodes*) together with a set E of ordered pairs of elements of V called *edges* (or *arcs*). The vertex a is called the *initial vertex* of the edge (a,b), and the vertex b is called the *terminal vertex* of this edge.

- An edge of the form (a,a) is called a *loop*.

Example: A drawing of the directed graph with vertices a, b, c, and d, and edges (a, b), (a, d), (b, b), (b, d), $(c,$ a$)$, (c, b), and (d, b) is shown here.



Representing Relations Using Matrices

- A relation between finite sets can be represented using a zero-one matrix.
- Suppose R is a relation from $A = \{a_1, a_2, \ldots, a_m\}$ to $B = \{b_1, b_2, \ldots, b_n\}$.
  - The elements of the two sets can be listed in any particular arbitrary order. When $A = B$, we use the same ordering.
- The relation R is represented by the matrix $M_R = [m_{ij}]$, where

$$m_{ij} = \begin{cases} 1 \text{ if } (a_i, b_j) \in R, \\ 0 \text{ if } (a_i, b_j) \notin R. \end{cases}$$

- The matrix representing R has a 1 as its (i,j) entry when a_i is related to b_j and a 0 if a_i is not related to b_j.

Examples of Representing Relations Using Matrices

Example 1: Suppose that $A = \{1,2,3\}$ and $B = \{1,2\}$. Let R be the relation from A to B containing (a,b) if $a \in A$, $b \in B$, and $a > b$. What is the matrix representing R (assuming the ordering of elements is the same as the increasing numerical order)?

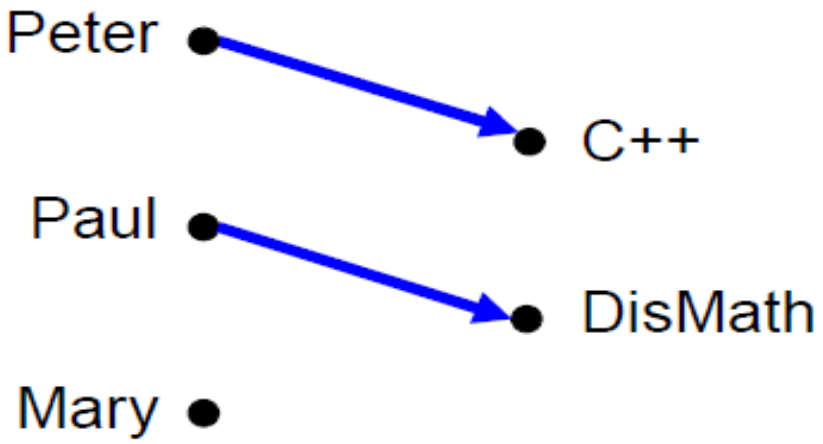
Solution: Because $R = \{(2,1), (3,1),(3,2)\}$, the matrix is

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

Binary Relations

EXAMPLE #1: (cont.)

- Peter R C++, Peter $\not R$ DisMath
  Paul $\not R$ C++, Paul R DisMath
  Mary $\not R$ C++, Mary $\not R$ DisMath



Directed Graph

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Matrix

Binary Relation on a Set

Definition: A binary relation *R on a set A* is a subset of $A \times A$ or a relation from A to A.

Example:

- Suppose that $A = \{a,b,c\}$. Then $R = \{(a,a),(a,b),(a,c)\}$ is a relation on A.
- Let $A = \{1, 2, 3, 4\}$. The ordered pairs in the relation $R = \{(a,b) \mid a \text{ divides } b\}$ are

  $\{(1,1), (1, 2), (1,3), (1, 4), (2, 2), (2, 4), (3, 3), \text{and } (4, 4)\}$.

REMARK:

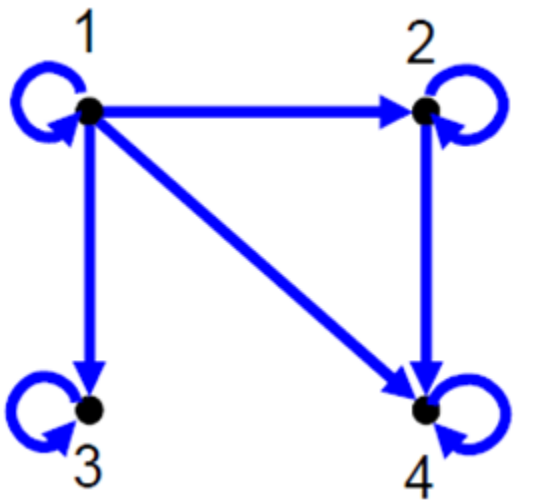
For any set A

1. $A \times A$ is known as the universal relation.
2. $\emptyset$ is known as the empty relation.

Binary Relation on a Set

- Let A be the set {1, 2, 3, 4}, which ordered pairs are in the relation R = {(a, b) | a divides b}?

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



$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Relations and Their Properties

Binary Relation on a Set (*cont.*)

Question: How many different relations are there on a set A with n elements?

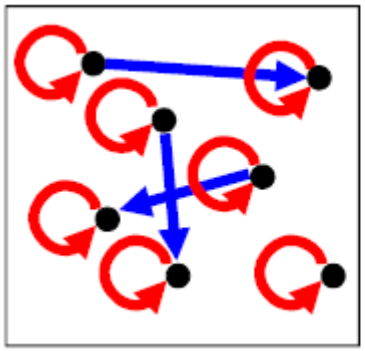
Solution:

- Suppose A has n elements
- Recall, a relation on a set A is a subset of A x A.
- A x A has n^2 elements.
- If a set has m element, its has 2^m subsets.
- Therefore, the answer is 2^{n^2}.

Reflexive Relations

Definition: R is *reflexive* iff $(a,a) \in R$ for every element $a \in A$. Written symbolically, R is reflexive if and only if

$$\forall a[a \in U \longrightarrow (a,a) \in R]$$



Reflexive

$\forall a\ ((a, a) \in R)$

Every node has a self-loop

$$\begin{pmatrix} 1 & ? & & \\ & 1 & & \\ & & 1 & \\ ? & & & 1 \end{pmatrix}$$

Reflexive

$\forall a\ ((a, a) \in R)$

All 1's on diagonal

If $A = \emptyset$ then the empty relation is reflexive vacuously. That is the empty relation on an empty set is reflexive!

Reflexive Relations

EXAMPLE: Let A = {1, 2, 3, 4} and determine whether relations R1, R2, R3, and R4 are Reflexive?

$R1 = \{(1, 1), (3, 3), (2, 2), (4, 4)\}$

$R2 = \{(1, 1), (1, 4), (2, 2), (3, 3), (4, 3)\}$

$R3 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$

$R4 = \{(1, 3), (2, 2), (2, 4), (3, 1), (4, 4)\}$

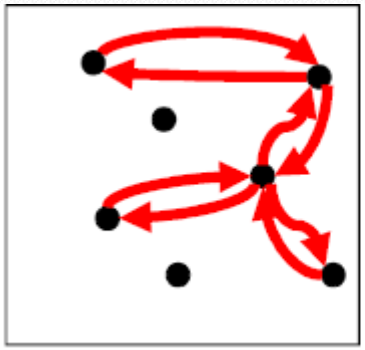
Solution:

- R1 is reflexive, since $(a, a) \in R1$ for all $a \in A$.
- R2 is not reflexive, because $(4, 4) \notin R2$.
- R3 is reflexive, since $(a, a) \in R3$ for all $a \in A$.
- R4 is not reflexive, because $(1, 1) \notin R4$, $(3, 3) \notin R4$.

Symmetric Relations

Definition: R is *symmetric* iff $(b,a) \in R$ whenever $(a,b) \in R$ for all $a,b \in A$. Written symbolically, R is symmetric if and only if

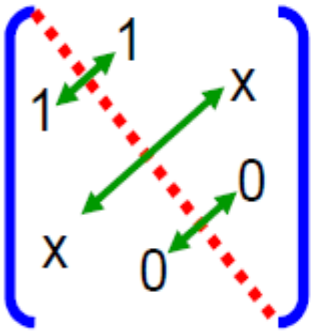
$$\forall a \forall b\, [(a,b) \in R \longrightarrow (b,a) \in R]$$



Symmetric

$\forall a\ \forall b\ (((a, b) \in R) \rightarrow ((b, a) \in R))$

Every link is bidirectional



Symmetric

$\forall a\ \forall b\ (((a, b) \in R) \rightarrow ((b, a) \in R))$

All identical across diagonal

Accordingly, R is symmetric if the elements in the ith row are the same as the elements in the ith column of the matrix M representing R. More precisely, M is a symmetric matrix
i.e. M = M^t

Symmetric Relations

EXAMPLE: Let A = {1, 2, 3, 4} and determine whether relations R1, R2, R3, and R4 are Symmetric?

$R1 = \{(1, 1), (1, 3), (2, 4), (3, 1), (4,2)\}$

$R2 = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$

$R3 = \{(2, 2), (2, 3), (3, 4)\}$

$R4 = \{(1, 1), (2, 2), (3, 3), (4, 3), (4, 4)\}$

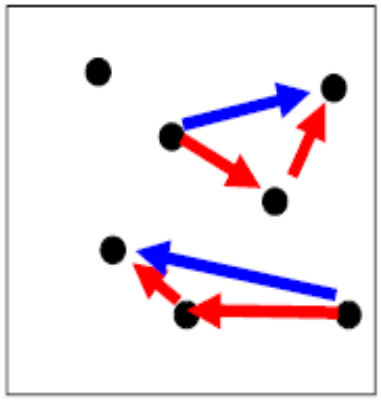
Solution:

- R1 is Symmetric, since (a, b) and (b, a) $\in$R1 for all (a, b) $\in$A.
- R2 is also symmetric. We say it is vacuously true.
- R3 is not symmetric, because (2,3) $\in$ R3 but (3,2) $\notin$ R3.
- R4 is not symmetric because (4,3) $\in$ R4 but (3,4) $\notin$ R4.

Transitive Relations

Definition: A relation R on a set A is called transitive if whenever $(a,b) \in R$ and $(b,c) \in R$, then $(a,c) \in R$, for all $a,b,c \in A$. Written symbolically, R is transitive if and only if

$$\forall a \forall b \forall c[(a,b) \in R \wedge (b,c) \in \mathrm{R} \longrightarrow (a,c) \in R\,]$$



Transitive

$\forall a \forall b \forall c\ (\ ((a,b) \in R \wedge (b,c) \in R) \rightarrow ((a,c) \in R))$

Every two adjacent forms a triangle
(Not easy to observe in Graph)

Transitive

$\forall a \forall b \forall c\ (\ ((a,b) \in R \wedge (b,c) \in R) \rightarrow ((a,c) \in R))$

Not easy to observe in Matrix

For a transitive directed graph, whenever there is an arrow going from one point to the second, and from the second to the third, there is an arrow going directly from the first to the third.

Transitive Relations

EXAMPLE: Let A = {1, 2, 3, 4} and determine whether relations R1, R2 and R3 are Transitive?

$R1 = \{(1, 1), (1, 2), (1, 3), (2, 3)\}$

$R2 = \{(1, 2), (1, 4), (2, 3), (3, 4)\}$

$R3 = \{(2, 1), (2, 4), (2, 3), (3,4)\}$

Solution:

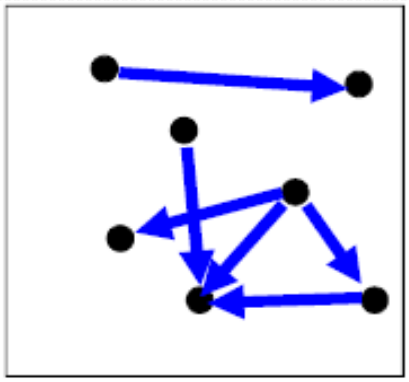
- R1 is transitive because (1, 1), (1, 2) are in R, then to be transitive relation(1,2) must be there and it belongs to R.
- R2 is not transitive since (1,2) and (2,3) $\in$ R2 but (1,3) $\notin$ R2.
- R3 is transitive.(check by definition)

Irreflexive Relations

Definition: R is irreflexive iff for all a∈A,(a,a) ∉R. That is, R is irreflexive if no element in A is related to itself by R.

Written symbolically, R is irreflexive if and only if

$$\forall a\,[(a \in A) \longrightarrow (a\,,\,a) \notin R]$$



Irreflexive

$\forall a\,((a \in A) \rightarrow ((a, a) \notin R))$

No node links to itself

R is not irreflexive iff there is an element a∈A such that (a,a) ∈R.

$$\begin{pmatrix} 0 & ? & \\ & 0 & \\ ? & & 0 \\ & & & 0 \end{pmatrix}$$

Irreflexive

$\forall a\,((a \in A) \rightarrow ((a, a) \notin R))$

All 0's on diagonal

Irreflexive Relations

EXAMPLE: Let A = {1, 2, 3, 4} and determine whether relations R1, R2 and R3 are Irreflexive?

$R1 = \{(1,3), (1,4), (2,3), (2,4), (3,1), (3,4)\}$

$R2 = \{(1,1), (1,2), (2,1), (2,2), (3,3), (4,4)\}$

$R3 = \{(1,2), (2,3), (3,3), (3,4)\}$

Solution:

- R1 is irreflexive since no element of A is related to itself in R1. i.e. $(1,1) \notin R1$, $(2,2) \notin R1$, $(3,3) \notin R1$, $(4,4) \notin R1$.
- R2 is not irreflexive, since all elements of A are related to themselves in R2.
- R3 is not irreflexive since $(3,3) \in R3$. Note that R3 is not reflexive.

Antisymmetric Relations

EXAMPLE: Let A = {1, 2, 3, 4} and determine whether relations R1, R2, R3, and R4 are Antisymmetric?

$R1 = \{(1,1),(2,2),(3,3)\}$

$R2 = \{(1,2),(2,2), (2,3), (3,4), (4,1)\}$

$R3=\{(1,3),(2,2), (2,4), (3,1), (4,2)\}$

$R4=\{(1,3),(2,4), (3,1), (4,3)\}$

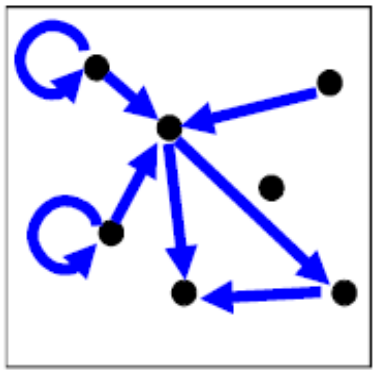
Solution:

- R1 is anti-symmetric and symmetric.
- R2 is anti-symmetric but not symmetric because $(1,2) \in R2$ but $(2,1) \notin R2$.
- R3 is not anti-symmetric since $(1,3)$ & $(3,1) \in R3$ but $1 \neq 3$. Note that R3 is symmetric.
- R4 is neither anti-symmetric because $(1,3)$ & $(3,1) \in R4$ but $1 \neq 3$ nor symmetric because $(2,4) \in R4$ but $(4,2) \notin R4$.

Antisymmetric Relations

Definition: A relation R on a set A such that for all $a,b \in A$ if $(a,b) \in R$ and $(b,a) \in R$, then $a = b$ is called *antisymmetric*. Written symbolically, R is antisymmetric if and only if $\forall a \forall b\,[(a,b) \in R \wedge (b,a) \in R \longrightarrow a = b]$

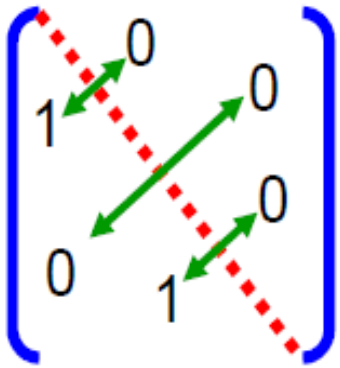
Note: (a,a) may be an element in R.



Antisymmetric

$\forall a\ \forall b\ (\ ((a, b) \in R \wedge (b, a) \in R) \rightarrow (a = b)\ )$

No link is bidirectional



Antisymmetric

$\forall a\ \forall b\ (\ ((a, b) \in R \wedge (b, a) \in R) \rightarrow (a = b)\ )$

All 1's are across from 0's

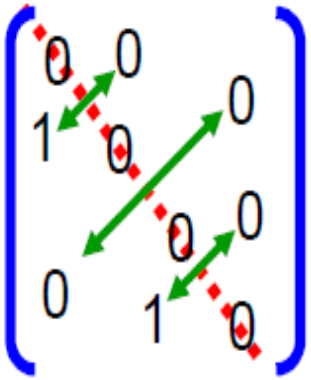
Let R be an anti-symmetric relation on a set A = {a1, a2, …, an}. Then if (ai, aj) ∈R for i ≠ j then (ai, aj) ∉R. Thus in the matrix representation of R there is a 1 in the ith row and jth column iff the jth row and ith column contains o vice versa.

Asymmetric Relations

Definition: R is Asymmetric iff for all $(a,b) \in R$ *than* $(b,a) \notin R$.
Written symbolically, R is Asymmetric if and only if

$$\forall a \forall b[((a,b) \in R)) \longrightarrow ((b,a) \notin R)]$$

Note:(a,a) cannot be an element in R.

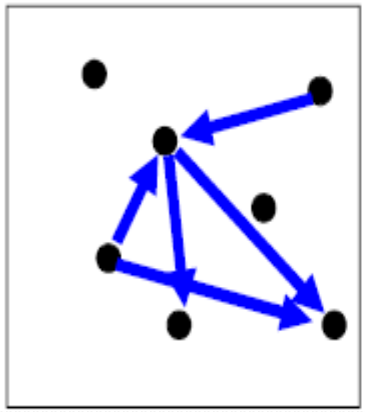


Asymmetric

$\forall a \forall b (((a, b) \in R) \rightarrow ((b, a) \notin R))$

All 1's are across from 0's (Antisymmetric)
All 0's on diagonal (Irreflexive)

Asymmetry = Antisymmetry + Irreflexivity



Asymmetric

$\forall a \forall b (((a, b) \in R) \rightarrow ((b, a) \notin R))$

No link is bidirectional (Antisymmetric)
No node links to itself (Irreflexive)

Asymmetric Relations

- **EXAMPLE**: Let A = {1, 2, 3, 4} and determine whether relations R1, R2 and R3 are Asymmetric?

  R1 = {(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)}

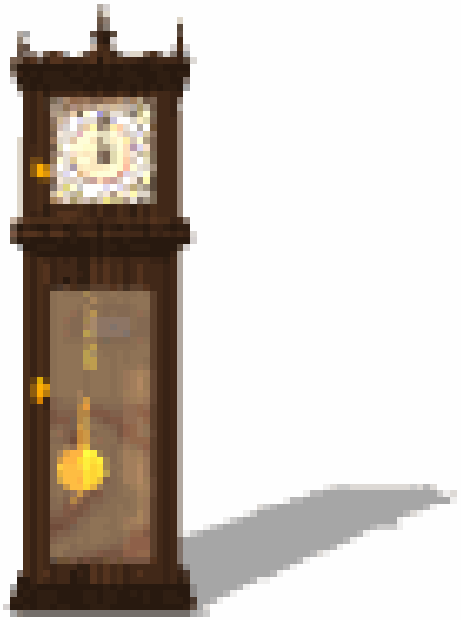
  R2 = {(1,2),(2,3),(3,4)}

  R3 = {(2,3),(3,3),(3,4)}

Solution:

- R1 is not Asymmetric since R1 is neither Antisymmetric nor Irreflexive.
- R2 is Asymmetric since R2 is both Antisymmetric and Irreflexive.
- R3 is not Asymmetric since it is Antisymmetric but not irreflexive.

Activity Time



Consider the following relations on {1, 2, 3, 4}:

$R1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$,

$R2 = \{(1, 1), (1, 2), (2, 1)\}$,

$R3 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\}$,

$R4 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$,

$R5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$,

$R6 = \{(3, 4)\}$.

Determine which of these relation are Reflexive, Symmetric, Transitive, Antisymmetric, Irreflexive and Asymmetric.

Combining Relations

As R is a subsets of A x B, the set operations can be applied

- Union (U)
- Intersection ($\cap$)
- Difference (-)
- Symmetric Complement ($\oplus$)

Given two relations R_1 and R_2, we can combine them using basic set operations to form new relations such as $R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 - R_2$, $R_2 - R_1$ and $R_1 \oplus R_2$.

Combining Relations

Given, $A = \{1,2,3\}$, $B = \{1,2,3,4\}$

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

$R_2 = \{(1,1),(1,2),(1,3),(1,4)\}$

- $R_1 \cup R_2 = \{(1,1),(1,2),(1,3),(1,4),(2,2),(3,3)\}$
- $R_1 \cap R_2 = \{(1,1)\}$
- $R_1 - R_2 = \{(2,2),(3,3)\}$
- $R_2 - R_1 = \{(1,2),(1,3),(1,4)\}$
- $R_1 \oplus R_2 = \{(1,2),(1,3),(1,4),(2,2),(3,3)\}$

Composition of Relations

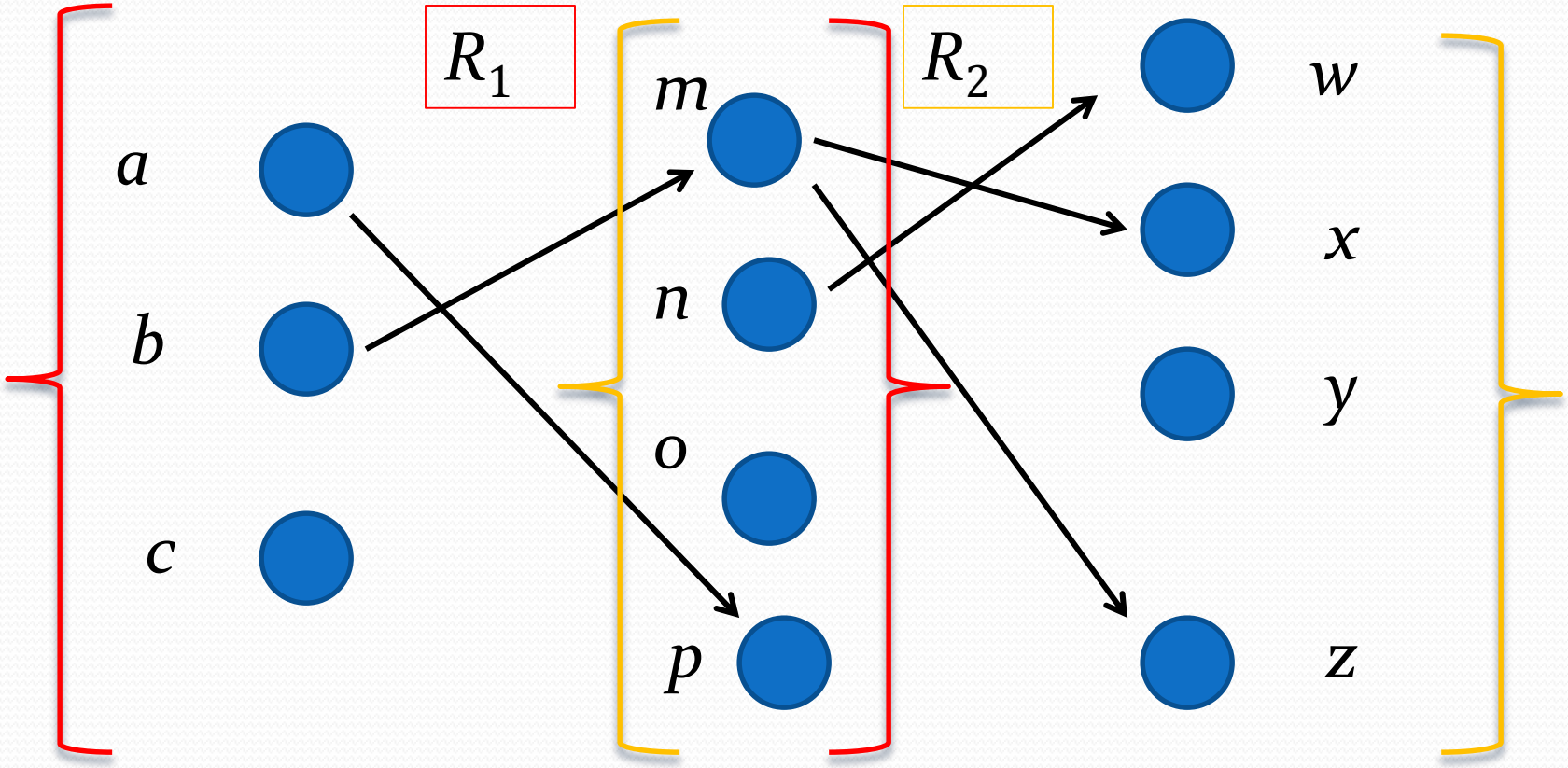
Definition: Suppose

- R_1 is a relation from a set A to a set B.
- R_2 is a relation from B to a set C.

Then the *composition* (or *composite*) of R_2 with R_1, is a relation from A to C where

- if (x,y) is a member of R_1 and (y,z) is a member of R_2, then (x,z) is a member of $R_2 \circ R_1$.

Representing the Composition of a Relation



$$R_1 \circ R_2 = \{(b,D),(b,B)\}$$

Composition of Relations

What is the composite of the relations R and S, where

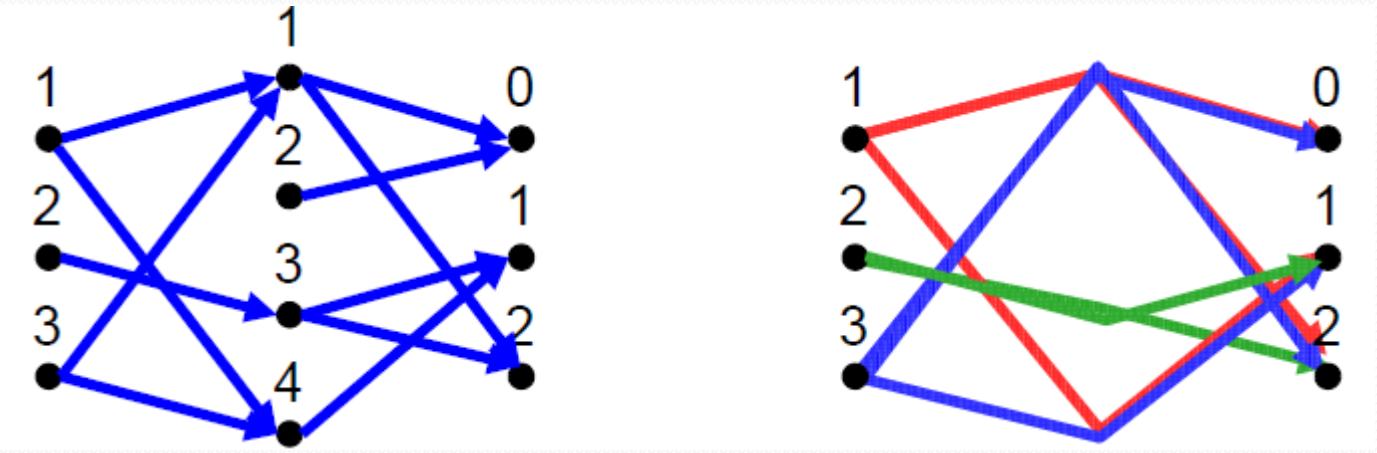
- R is the relation from **{1,2,3}** to **{1,2,3,4}** with

  R = {(1,1),(1,4),(2,3),(3,1),(3,4)}

- S is the relation from **{1,2,3,4}** to **{0,1,2}** with

  S = {(1,0),(1,2),(2,0),(3,1),(3,2),(4,1)}?

- S o R = {(1,0),(1,2),(1,1), (2,2),((2,1), 3,0),(3,2),(3,1)}



INVERSE OF A RELATION

Let R be a relation from A to B. The inverse relation R^{-1} from B to A is defined as:

$$R^{-1} = \{(b,a) \in B \times A \mid (a,b) \in R\}$$

More simply, the inverse relation R^{-1} of R is obtained by interchanging the elements of all the ordered pairs in R.

- **Example**

X = {a, b, c} and Y={1, 2}

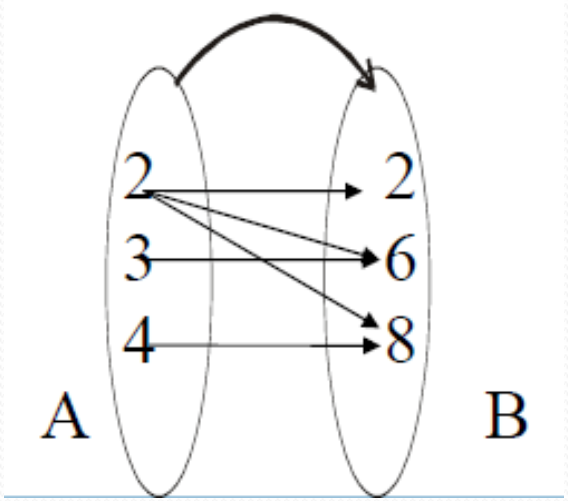
R = {(a, 1), (b, 2), (c, 1)}

- R^{-1} = {(1, a), (2, b), (1, c)}

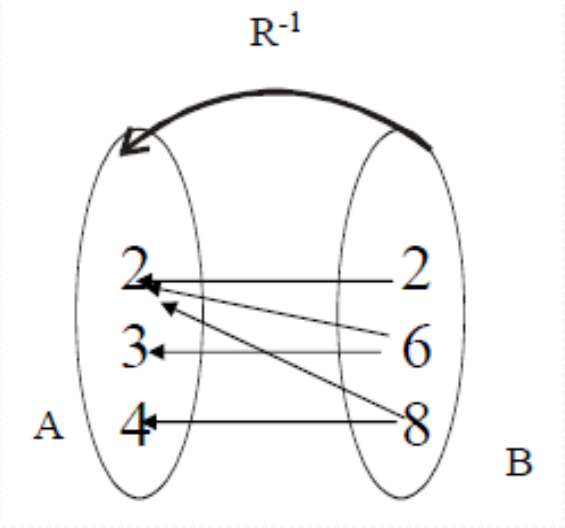
INVERSE OF A RELATION

The relation

R = {(2,2), (2,6), (2,8), (3,6), (4,8)} is represented by the arrow diagram.



Then inverse of the above relation can be obtained simply changing the directions of the arrows and hence the diagram is



Equivalence Relations

Equivalence Relations

Definition 1: A relation on a set A is called an *equivalence relation* if it is reflexive, symmetric, and transitive.

Definition 2: Two elements a, and b that are related by an equivalence relation are called *equivalent*. The notation $a \sim b$ is often used to denote that a and b are equivalent elements with respect to a particular equivalence relation.

Strings

Example:

Suppose that R is the relation on the set of strings of English letters such that aRb if and only if $l(a) = l(b)$, where $l(x)$ is the length of the string x. Is R an equivalence relation?

Solution: Show that all of the properties of an equivalence relation hold.

- *Reflexivity*: Because $l(a) = l(a)$, it follows that aRa for all strings a.
- *Symmetry*: Suppose that aRb. Since $l(a) = l(b)$, $l(b) = l(a)$ also holds and bRa.
- *Transitivity*: Suppose that aRb and bRc. Since $l(a) = l(b)$, and $l(b) = l(c)$, $l(a) = l(a)$ also holds and aRc.

Congruence Modulo m

Example: Let m be an integer with $m > 1$. Show that the relation

$R = \{(a,b) \mid a \equiv b \pmod{m}\}$

is an equivalence relation on the set of integers.

Solution: Recall that $a \equiv b \pmod{m}$ if and only if m divides $a - b$.

- *Reflexivity*: $a \equiv a \pmod{m}$ since $a - a = 0$ is divisible by m since $0 = 0 \cdot m$.
- *Symmetry*: Suppose that $a \equiv b \pmod{m}$. Then $a - b$ is divisible by m, and so $a - b = km$, where k is an integer. It follows that $b - a = (-k)\, m$, so $b \equiv a \pmod{m}$.
- *Transitivity*: Suppose that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then m divides both $a - b$ and $b - c$. Hence, there are integers k and l with $a - b = km$ *and* $b - c = lm$. We obtain by adding the equations:

  $$a - c = (a - b) + (b - c) = km + lm = (k + l)\, m.$$

  Therefore, $a \equiv c \pmod{m}$.

Divides

Example: Show that the "divides" relation on the set of positive integers is not an equivalence relation.

Solution: The properties of reflexivity, and transitivity do hold, but there relation is not transitive. Hence, "divides" is not an equivalence relation.

- *Reflexivity*: $a \mid a$ for all a.
- *Not Symmetric*: For example, $2 \mid 4$, but $4 \nmid 2$. Hence, the relation is not symmetric.
- *Transitivity*: Suppose that a divides b and b divides c. Then there are positive integers k and l such that $b = ak$ and $c = bl$. Hence, $c = a(kl)$, so a divides c. Therefore, the relation is transitive.

Partial Orderings

Partial Orderings

Definition 1: A relation R on a set S is called a *partial ordering*, or *partial order*, if it is reflexive, antisymmetric, and transitive.

A set together with a partial ordering R is called a *partially ordered set*, or *poset*, and is denoted by (S, R). Members of S are called *elements* of the poset.

Partial Orderings (*continued*)

Example 1: Show that the "greater than or equal" relation ($\geq$) is a partial ordering on the set of integers.

- *Reflexivity*: $a \geq a$ for every integer a.
- *Antisymmetry*: If $a \geq b$ and $b \geq a$, then $a = b$.
- *Transitivity*: If $a \geq b$ and $b \geq c$, then $a \geq c$.

These properties all follow from the order axioms for the integers. (*See Appendix* 1).

Partial Orderings (*continued*)

Example 2: Show that the divisibility relation (|) is a partial ordering on the set of integers.

- *Reflexivity*: $a \mid a$ for all integers a. (*see Example* 9 *in Section* 9.1)
- *Antisymmetry*: If a and b are positive integers with $a \mid b$ and $b \mid a$, then $a = b$. (*see Example* 12 *in Section* 9.1)
- *Transitivity*: Suppose that a divides b and b divides c. Then there are positive integers k and l such that $b = ak$ and $c = bl$. Hence, $c = a(kl)$, so a divides c. Therefore, the relation is transitive.

- $(\boldsymbol{Z}^+, |)$ is a poset.

Partial Orderings (*continued*)

Example 3: Show that the inclusion relation ($\subseteq$) is a partial ordering on the power set of a set S.

- *Reflexivity*: $A \subseteq A$ whenever A is a subset of S.
- *Antisymmetry*: If A and B are positive integers with $A \subseteq B$ and $B \subseteq A$, then $A = B$.
- *Transitivity*: If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

The properties all follow from the definition of set inclusion.

Number Theory and Cryptography

Chapter 4

Chapter Motivation

- *Number theory* is the part of mathematics devoted to the study of the integers and their properties.
- Key ideas in number theory include divisibility and the primality of integers.
- Number theory has long been studied because of the beauty of its ideas, its accessibility, and its wealth of open questions.
- We'll use many ideas developed in Chapter 1 about proof methods and proof strategy in our exploration of number theory.
- Mathematicians have long considered number theory to be pure mathematics, but it has important applications to computer science and cryptography studied in Sections 4.5 and 4.6.

Chapter Summary

- Divisibility and Modular Arithmetic
- Primes and Greatest Common Divisors
- Solving Congruencies
- Applications of Congruencies
- Cryptography

Divisibility and Modular Arithmetic

Section 4.1

Section Summary

- Division
- Division Algorithm
- Modular Arithmetic

Division

Definition: If a and b are integers with $a \neq 0$, then a *divides* b if there exists an integer c such that $b = ac$.

- When a divides b we say that a is a *factor* or *divisor* of b and that b is a multiple of a.
- The notation $a \mid b$ denotes that a divides b.
- If $a \mid b$, then b/a is an integer.
- If a does not divide b, we write $a \nmid b$.

Example: Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Properties of Divisibility

Theorem 1: Let a, b, and c be integers, where $a \neq 0$.

i. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
ii. If $a \mid b$, then $a \mid bc$ for all integers c;
iii. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: (i) Suppose $a \mid b$ and $a \mid c$, then it follows that there are integers s and t with $b = as$ and $c = at$. Hence,

$b + c = as + at = a(s + t)$. Hence, $a \mid (b + c)$

(Exercises 3 and 4 ask for proofs of parts (ii) and (iii).) ◄

Corollary: If a, b, and c be integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

Can you show how it follows easily from from (ii) and (i) of Theorem 1?

Division Algorithm

- When an integer is divided by a positive integer, there is a quotient and a remainder. This is traditionally called the "Division Algorithm," but is really a theorem.

Division Algorithm: If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$ (*proved in Section* 5.2).

- d is called the *divisor*.
- a is called the *dividend*.
- q is called the *quotient*.
- r is called the *remainder*.

Definitions of Functions **div** and **mod**

$q = a$ **div** d

$r = a$ **mod** d

Examples:

- What are the quotient and remainder when 101 is divided by 11?

  Solution: The quotient when 101 is divided by 11 is 9 = 101 **div** 11, and the remainder is 2 = 101 **mod** 11.

- What are the quotient and remainder when −11 is divided by 3?

  Solution: The quotient when −11 is divided by 3 is −4 = −11 **div** 3, and the remainder is 1 = −11 **mod** 3.

Congruence Relation

Definition: If a and b are integers and m is a positive integer, then a is *congruent* to b *modulo* m if m divides $a - b$.

- The notation $a \equiv b \pmod{m}$ says that a is congruent to b modulo m.
- We say that $a \equiv b \pmod{m}$ is a *congruence* and that m is its *modulus*.
- Two integers are congruent mod m if and only if they have the same remainder when divided by m.
- If a is not congruent to b modulo m, we write

$$a \not\equiv b \pmod{m}$$

Example: Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Solution:

- $17 \equiv 5 \pmod{6}$ because 6 divides $17 - 5 = 12$.
- $24 \not\equiv 14 \pmod{6}$ since 6 divides $24 - 14 = 10$ is not divisible by 6.

More on Congruences

Theorem 4: Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof:

- If $a \equiv b \pmod{m}$, then (by the definition of congruence) $m \mid a - b$. Hence, there is an integer k such that $a - b = km$ and equivalently $a = b + km$.
- Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, $m \mid a - b$ and $a \equiv b \pmod{m}$. ◀

The Relationship between (mod m) and **mod** m Notations

- The use of "mod" in $a \equiv b \pmod{m}$ and $a \bmod m = b$ are different.
  - $a \equiv b \pmod{m}$ is a relation on the set of integers.
  - In $a \bmod m = b$, the notation **mod** denotes a function.
- The relationship between these notations is made clear in this theorem.
- **Theorem 3**: Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$. (*Proof in the exercises*)

Congruencies of Sums and Products

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \text{ and } ac \equiv bd \pmod{m}$$

Example: Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows from Theorem 5 that

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$$

$$77 = 7\ 11 \equiv 2 + 1 = 3 \pmod{5}$$

Algebraic Manipulation of Congruencies

- Multiplying both sides of a valid congruence by an integer preserves validity.

  If $a \equiv b \pmod{m}$ holds then $c \cdot a \equiv c \cdot b \pmod{m}$, where c is any integer, holds by Theorem 5 with $d = c$.

- Adding an integer to both sides of a valid congruence preserves validity.

  If $a \equiv b \pmod{m}$ holds then $c + a \equiv c + b \pmod{m}$, where c is any integer, holds by Theorem 5 with $d = c$.

- Dividing a congruence by an integer does not always produce a valid congruence.

  Example: The congruence $14 \equiv 8 \pmod{6}$ holds. But dividing both sides by 2 does not produce a valid congruence since $14/2 = 7$ and $8/2 = 4$, but $7 \not\equiv 4 \pmod{6}$.

Computing the **mod** *m* Function of Products and Sums

- We use the following corollary to Theorem 5 to compute the remainder of the product or sum of two integers when divided by *m* from the remainders when each is divided by *m*.

Corollary: Let *m* be a positive integer and let *a* and *b* be integers. Then

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

and

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

(*proof in text*)

Applications of Congruences

Section Summary

- Hashing Functions
- Pseudorandom Numbers
- Check Digits

Hashing Functions

Definition: A *hashing function h* assigns memory location $h(k)$ to the record that has k as its key.

- A common hashing function is $h(k) = k$ **mod** m, where m is the number of memory locations.
- Because this hashing function is onto, all memory locations are possible.

Example: Let $h(k) = k$ **mod** 111. This hashing function assigns the records of customers with social security numbers as keys to memory locations in the following manner:

h(064212848) = 064212848 **mod** 111 = 14

h(037149212) = 037149212 **mod** 111 = 65

h(107405723) = 107405723 **mod** 111 = 14, but since location 14 is already occupied, the record is assigned to the next available position, which is 15.

- The hashing function is not one-to-one as there are many more possible keys than memory locations. When more than one record is assigned to the same location, we say a *collision* occurs. Here a collision has been resolved by assigning the record to the first free location.
- For collision resolution, we can use a *linear probing function*:

  $h(k,i) = (h(k) + i)$ **mod** m, where i runs from 0 to $m - 1$.
- There are many other methods of handling with collisions. You may cover these in a later CS course.

Pseudorandom Numbers

- Randomly chosen numbers are needed for many purposes, including computer simulations.
- *Pseudorandom numbers* are not truly random since they are generated by systematic methods.
- The *linear congruential method* is one commonly used procedure for generating pseudorandom numbers.
- Four integers are needed: the *modulus* m, the *multiplier* a, the *increment* c, and *seed* x_0, with $2 \leq a < m$, $0 \leq c < m$, $0 \leq x_0 < m$.
- We generate a sequence of pseudorandom numbers $\{x_n\}$, with $0 \leq x_n < m$ for all n, by successively using the recursively defined function

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

(*an example of a recursive definition, discussed in Section* 5.3*)*

- If psudorandom numbers between 0 and 1 are needed, then the generated numbers are divided by the modulus, x_n / m.

Pseudorandom Numbers

- **Example**: Find the sequence of pseudorandom numbers generated by the linear congruential method with modulus $m = 9$, multiplier $a = 7$, increment $c = 4$, and seed $x_0 = 3$.
- **Solution**: Compute the terms of the sequence by successively using the congruence $x_{n+1} = (7x_n + 4) \bmod 9$, with $x_0 = 3$.

$x_1 = 7x_0 + 4 \bmod 9 = 7 \cdot 3 + 4 \bmod 9 = 25 \bmod 9 = 7,$
$x_2 = 7x_1 + 4 \bmod 9 = 7 \cdot 7 + 4 \bmod 9 = 53 \bmod 9 = 8,$
$x_3 = 7x_2 + 4 \bmod 9 = 7 \cdot 8 + 4 \bmod 9 = 60 \bmod 9 = 6,$
$x_4 = 7x_3 + 4 \bmod 9 = 7 \cdot 6 + 4 \bmod 9 = 46 \bmod 9 = 1,$
$x_5 = 7x_4 + 4 \bmod 9 = 7 \cdot 1 + 4 \bmod 9 = 11 \bmod 9 = 2,$
$x_6 = 7x_5 + 4 \bmod 9 = 7 \cdot 2 + 4 \bmod 9 = 18 \bmod 9 = 0,$
$x_7 = 7x_6 + 4 \bmod 9 = 7 \cdot 0 + 4 \bmod 9 = 4 \bmod 9 = 4,$
$x_8 = 7x_7 + 4 \bmod 9 = 7 \cdot 4 + 4 \bmod 9 = 32 \bmod 9 = 5,$
$x_9 = 7x_8 + 4 \bmod 9 = 7 \cdot 5 + 4 \bmod 9 = 39 \bmod 9 = 3.$

The sequence generated is 3,7,8,6,1,2,0,4,5,3,7,8,6,1,2,0,4,5,3,...

It repeats after generating 9 terms.

- Commonly, computers use a linear congruential generator with increment $c = 0$. This is called a *pure multiplicative generator*. Such a generator with modulus $2^{31} - 1$ and multiplier $7^5 = 16{,}807$ generates $2^{31} - 2$ numbers before repeating.

Check Digits: UPCs

- A common method of detecting errors in strings of digits is to add an extra digit at the end, which is evaluated using a function. If the final digit is not correct, then the string is assumed not to be correct.

Example: Retail products are identified by their *Universal Product Codes* (*UPC*s). Usually these have 12 decimal digits, the last one being the check digit. The check digit is determined by the congruence:

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}.$$

a. Suppose that the first 11 digits of the UPC are 79357343104. What is the check digit?

b. Is 041331021641 a valid UPC?

Solution:

a. $3\cdot 7 + 9 + 3\cdot 3 + 5 + 3\cdot 7 + 3 + 3\cdot 4 + 3 + 3\cdot 1 + 0 + 3\cdot 4 + x_{12} \equiv 0 \pmod{10}$

$21 + 9 + 9 + 5 + 21 + 3 + 12 + 3 + 3 + 0 + 12 + x_{12} \equiv 0 \pmod{10}$

$98 + x_{12} \equiv 0 \pmod{10}$

$x_{12} \equiv 0 \pmod{10}$ So, the check digit is 2.

b. $3\cdot 0 + 4 + 3\cdot 1 + 3 + 3\cdot 3 + 1 + 3\cdot 0 + 2 + 3\cdot 1 + 6 + 3\cdot 4 + 1 \equiv 0 \pmod{10}$

$0 + 4 + 3 + 3 + 9 + 1 + 0 + 2 + 3 + 6 + 12 + 1 = 44 \equiv 4 \not\equiv \pmod{10}$

Hence, 041331021641 is not a valid UPC.

Check Digits:ISBNs

Books are identified by an *International Standard Book Number* (ISBN-10), a 10 digit code. The first 9 digits identify the language, the publisher, and the book. The tenth digit is a check digit, which is determined by the following congruence

$$x_{10} \equiv \sum_{i=1}^{9} i x_i \pmod{11}.$$

The validity of an ISBN-10 number can be evaluated with the equivalent $\sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}$.

a. Suppose that the first 9 digits of the ISBN-10 are 007288008. What is the check digit?

b. Is 084930149X a valid ISBN10?

Solution:

a. $X_{10} \equiv 1\cdot 0 + 2\cdot 0 + 3\cdot 7 + 4\cdot 2 + 5\cdot 8 + 6\cdot 8 + 7\cdot 0 + 8\cdot 0 + 9\cdot 8 \pmod{11}$.
$X_{10} \equiv 0 + 0 + 21 + 8 + 40 + 48 + 0 + 0 + 72 \pmod{11}$.
$X_{10} \equiv 189 \equiv 2 \pmod{11}$. Hence, $X_{10} = 2$.

X is used for the digit 10.

b. $1\cdot 0 + 2\cdot 8 + 3\cdot 4 + 4\cdot 9 + 5\cdot 3 + 6\cdot 0 + 7\cdot 1 + 8\cdot 4 + 9\cdot 9 + 10\cdot 10 =$
$0 + 16 + 12 + 36 + 15 + 0 + 7 + 32 + 81 + 100 = 299 \equiv 2 \not\equiv 0 \pmod{11}$
Hence, 084930149X is not a valid ISBN-10.

- A *single error* is an error in one digit of an identification number and a *transposition error* is the accidental interchanging of two digits. Both of these kinds of errors can be detected by the check digit for ISBN-10. (*see text for more details*)

Arithmetic Modulo *m*

Definitions: Let $\mathbf{Z}_m$ be the set of nonnegative integers less than m: $\{0,1, \ldots, m-1\}$

- The operation $+_m$ is defined as $a +_m b = (a + b)$ **mod** m. This is *addition modulo m*.
- The operation $\cdot_m$ is defined as $a \cdot_m b = (a \,.\, b)$ **mod** m. This is *multiplication modulo m*.
- Using these operations is said to be doing *arithmetic modulo m*.

Example: Find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution: Using the definitions above:

- $7 +_{11} 9 = (7 + 9)$ **mod** $11 = 16$ **mod** $11 = 5$
- $7 \cdot_{11} 9 = (7 \cdot 9)$ **mod** $11 = 63$ **mod** $11 = 8$

Arithmetic Modulo *m*

- The operations $+_m$ and $\cdot_m$ satisfy many of the same properties as ordinary addition and multiplication.
  - *Closure*: If a and b belong to $\mathbf{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\mathbf{Z}_m$.
  - *Associativity*: If a, b, and c belong to $\mathbf{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
  - *Commutativity*: If a and b belong to $\mathbf{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
  - *Identity elements*: The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively.
    - If a belongs to $\mathbf{Z}_m$, then $a +_m 0 = a$ and $a \cdot_m 1 = a$.

continued →

Arithmetic Modulo *m*

- *Additive inverses*: If $a \neq 0$ belongs to $\mathbf{Z}_m$, then $m - a$ is the additive inverse of a modulo m and o is its own additive inverse.
  - $a +_m (m - a) = 0$ and $0 +_m 0 = 0$
- *Distributivity*: If a, b, and c belong to $\mathbf{Z}_m$, then
  - $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.
- Exercises 42-44 ask for proofs of these properties.
- Multiplicatative inverses have not been included since they do not always exist. For example, there is no multiplicative inverse of 2 modulo 6.
- (*optional*) Using the terminology of abstract algebra, $\mathbf{Z}_m$ with $+_m$ is a commutative group and $\mathbf{Z}_m$ with $+_m$ and $\cdot_m$ is a commutative ring.

Primes and Greatest Common Divisors

Section 4.3

Section Summary

- Prime Numbers and their Properties
- Greatest Common Divisors and Least Common Multiples
- The Euclidian Algorithm
- gcds as Linear Combinations

Primes

Definition: A positive integer *p* greater than 1 is called *prime* if the only positive factors of *p* are 1 and *p*. A positive integer that is greater than 1 and is not prime is called *composite*.

Example: The integer 7 is prime because its only positive factors are 1 and 7, but 9 is composite because it is divisible by 3.

The Fundamental Theorem of Arithmetic

Theorem: Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of non decreasing size.

Examples:

- $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
- $641 = 641$
- $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
- $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

The Sieve of Erastosthenes

TABLE 1 The Sieve of Eratosthenes.

Integers divisible by 2 other than 2 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 3 other than 3 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 5 other than 5 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

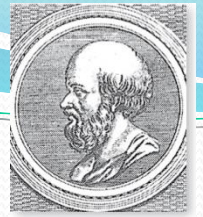
Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

If an integer n is a composite integer, then it has a prime divisor less than or equal to $\sqrt{n}$.

To see this, note that if $n = ab$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Trial division, a very inefficient method of determining if a number n is prime, is to try every integer $i \leq \sqrt{n}$ and see if n is divisible by i.



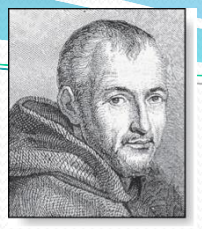
Erastothenes
(276-194 B.C.)

The Sieve of Erastosthenes

- The *Sieve of Erastosthenes* can be used to find all primes not exceeding a specified positive integer. For example, begin with the list of integers between 1 and 100.
  a. Delete all the integers, other than 2, divisible by 2.
  b. Delete all the integers, other than 3, divisible by 3.
  c. Next, delete all the integers, other than 5, divisible by 5.
  d. Next, delete all the integers, other than 7, divisible by 7.
  e. Since all the remaining integers are not divisible by any of the previous integers, other than 1, the primes are:

{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89, 97}

continued →



Marin Mersenne
(1588-1648)

Mersenne Primes

Definition: Prime numbers of the form $2^p - 1$, where p is prime, are called *Mersenne primes*.

- $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 37$, and $2^7 - 1 = 127$ are Mersenne primes.
- $2^{11} - 1 = 2047$ is not a Mersenne prime since $2047 = 23 \cdot 89$.
- There is an efficient test for determining if $2^p - 1$ is prime.
- The largest known prime numbers are Mersenne primes.
- As of mid 2011, 47 Mersenne primes were known, the largest is $2^{43,112,609} - 1$, which has nearly 13 million decimal digits.
- The *Great Internet Mersenne Prime Search* (*GIMPS*) is a distributed computing project to search for new Mersenne Primes.

http://www.mersenne.org/

Greatest Common Divisor

Definition: Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and also $d \mid b$ is called the greatest common divisor of a and b. The greatest common divisor of a and b is denoted by $\gcd(a,b)$.

One can find greatest common divisors of small numbers by inspection.

Example: What is the greatest common divisor of 24 and 36?

Solution: $\gcd(24,36) = 12$

Example: What is the greatest common divisor of 17 and 22?

Solution: $\gcd(17,22) = 1$

Greatest Common Divisor

Definition: The integers a and b are *relatively prime* if their greatest common divisor is 1.

Example: 17 and 22

Definition: The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Example: Determine whether the integers 10, 17 and 21 are pairwise relatively prime.

Solution: Because $\gcd(10,17) = 1$, $\gcd(10,21) = 1$, and $\gcd(17,21) = 1$, 10, 17, and 21 are pairwise relatively prime.

Example: Determine whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution: Because $\gcd(10,24) = 2$, 10, 19, and 24 are not pairwise relatively prime.

Finding the Greatest Common Divisor Using Prime Factorizations

- Suppose the prime factorizations of a and b are:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} , \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n} ,$$

where each exponent is a nonnegative integer, and where all primes occurring in either prime factorization are included in both. Then:

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)} .$$

- This formula is valid since the integer on the right (of the equals sign) divides both a and b. No larger integer can divide both a and b.

Example: $120 = 2^3 \cdot 3 \cdot 5$ $\quad 500 = 2^2 \cdot 5^3$

$\gcd(120,500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 3^0 \cdot 5^1 = 20$

- Finding the gcd of two positive integers using their prime factorizations is not efficient because there is no efficient algorithm for finding the prime factorization of a positive integer.

Least Common Multiple

Definition: The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by $\text{lcm}(a,b)$.

- The least common multiple can also be computed from the prime factorizations.

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

This number is divided by both a and b and no smaller number is divided by a and b.

Example: $\text{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)}\, 3^{\max(5,3)}\, 7^{\max(2,0)} = 2^4\, 3^5\, 7^2$

- The greatest common divisor and the least common multiple of two integers are related by:

Theorem 5: Let a and b be positive integers. Then

$$ab = \gcd(a,b) \cdot \text{lcm}(a,b)$$

(*proof is Exercise* 31)

Euclidean Algorithm

Euclid
(325 B.C.E. – 265 B.C.E.)

- The Euclidian algorithm is an efficient method for computing the greatest common divisor of two integers. It is based on the idea that gcd(a,b) is equal to gcd(a,c) when $a > b$ and c is the remainder when a is divided by b.

Example: Find gcd(91, 287):

- $287 = 91 \cdot 3 + 14$
- $91 = 14 \cdot 6 + 7$
- $14 = 7 \cdot 2 + 0$

Divide 287 by 91

Divide 91 by 14

Divide 14 by 7

Stopping condition

$$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$$

continued →

Euclidean Algorithm

- The Euclidean algorithm expressed in pseudocode is:

```
procedure gcd(a, b: positive integers)
x := a
x := b
while   y ≠ 0
      r := x mod y
      x := y
      y := r
return x {gcd(a,b) is x}
```

- In Section 5.3, we'll see that the time complexity of the algorithm is $O(\log b)$, where $a > b$.

Étienne Bézout
(1730-1783)

gcds as Linear Combinations

Bézout's Theorem: If a and b are positive integers, then there exist integers s and t such that $\gcd(a,b) = sa + tb$.

Definition: If a and b are positive integers, then integers s and t such that $\gcd(a,b) = sa + tb$ are called *Bézout coefficients* of a and b. The equation $\gcd(a,b) = sa + tb$ is called *Bézout's identity*.

- By Bézout's Theorem, the gcd of integers a and b can be expressed in the form $sa + tb$ where s and t are integers. This is a *linear combination* with integer coefficients of a and b.
  - $\gcd(6,14) = (-2)\cdot 6 + 1\cdot 14$

Finding gcds as Linear Combinations

Example: Express gcd(252,198) = 18 as a linear combination of 252 and 198.

Solution: First use the Euclidean algorithm to show gcd(252,198) = 18

i. $252 = 1 \cdot 198 + 54$
ii. $198 = 3 \cdot 54 + 36$
iii. $54 = 1 \cdot 36 + 18$
iv. $36 = 2 \cdot 18$

- Now working backwards, from iii and i above
  - $18 = 54 - 1 \cdot 36$
  - $36 = 198 - 3 \cdot 54$
- Substituting the 2nd equation into the 1st yields:
  - $18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$
- Substituting $54 = 252 - 1 \cdot 198$ (from i)) yields:
  - $18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$

- This method illustrated above is a two pass method. It first uses the Euclidian algorithm to find the gcd and then works backwards to express the gcd as a linear combination of the original two integers. A one pass method, called the *extended Euclidean algorithm*, is developed in the exercises.

Dividing Congruencies by an Integer

- Dividing both sides of a valid congruence by an integer does not always produce a valid congruence (see Section 4.1).
- But dividing by an integer relatively prime to the modulus does produce a valid congruence:

Theorem 7: Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c,m) = 1$, then $a \equiv b \pmod{m}$.

Proof: Since $ac \equiv bc \pmod{m}$, $m \mid ac - bc = c(a - b)$ by Lemma 2 and the fact that $\gcd(c,m) = 1$, it follows that $m \mid a - b$. Hence, $a \equiv b \pmod{m}$. ◀

Solving Congruencies

Section 4.4

Section Summary

- Linear Congruencies
- The Chinese Remainder Theorem
- Fermat's Little Theorem
- Pseudo primes

Linear Congruencies

Definition: A congruence of the form

$$ax \equiv b \pmod{m},$$

where m is a positive integer, a and b are integers, and x is a variable, is called a *linear congruence*.

- The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence.

Definition: An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an *inverse* of a modulo m.

Example: 5 is an inverse of 3 modulo 7 since $5 \cdot 3 = 15 \equiv 1 \pmod{7}$

- One method of solving linear congruencies makes use of an inverse $\bar{a}$, if it exists. Although we can not divide both sides of the congruence by a, we can multiply by $\bar{a}$ to solve for x.

Inverse of a modulo m

- The following theorem guarantees that an inverse of a modulo m exists whenever a and m are relatively prime. Two integers a and b are relatively prime when $\gcd(a,b) = 1$.

Theorem 1: If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m. (This means that there is a unique positive integer $\bar{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\bar{a}$ modulo m.)

Proof: Since $\gcd(a,m) = 1$, by Theorem 6 of Section 4.3, there are integers s and t such that $sa + tm = 1$.

- Hence, $sa + tm \equiv 1 \pmod{m}$.
- Since $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$
- Consequently, s is an inverse of a modulo m.
- The uniqueness of the inverse is Exercise 7.

◀

Finding Inverses

- The Euclidean algorithm and Bézout coefficients gives us a systematic approaches to finding inverses.

  Example: Find an inverse of 3 modulo 7.

  Solution: Because gcd(3,7) = 1, by Theorem 1, an inverse of 3 modulo 7 exists.

  - Using the Euclidian algorithm: $7 = 2 \cdot 3 + 1$.
  - From this equation, we get $-2 \cdot 3 + 1 \cdot 7 = 1$, and see that -2 and 1 are Bézout coefficients of 3 and 7.
  - Hence, -2 is an inverse of 3 modulo 7.
  - Also every integer congruent to -2 modulo 7 is an inverse of 3 modulo 7, i.e., 5, -9, 12, etc.

Finding Inverses

Example: Find an inverse of 101 modulo 4620.

Solution: First use the Euclidian algorithm to show that gcd(101,4620) = 1.

$4620 = 45 \cdot 101 + 75$
$101 = 1 \cdot 75 + 26$
$75 = 2 \cdot 26 + 23$
$26 = 1 \cdot 23 + 3$
$23 = 7 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 2 \cdot 1$

Since the last nonzero remainder is 1, gcd(101,4260) = 1

Working Backwards:

$1 = 3 - 1 \cdot 2$
$1 = 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$
$1 = -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$
$1 = 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75$
$1 = 26 \cdot (101 - 1 \cdot 75) - 9 \cdot 75$
$= 26 \cdot 101 - 35 \cdot 75$
$1 = 26 \cdot 101 - 35 \cdot (42620 - 45 \cdot 101)$
$= -35 \cdot 42620 + 1601 \cdot 101$

Bézout coefficients : -35 and 1601

1601 is an inverse of 101 modulo 42620

Using Inverses to Solve Congruences

- We can solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides by $\bar{a}$.

Example: What are the solutions of the congruence $3x \equiv 4 \pmod{7}$.

Solution: We found that -2 is an inverse of 3 modulo 7 (two slides back). We multiply both sides of the congruence by -2 giving

$$-2 \cdot 3x \equiv -2 \cdot 4 \pmod{7}.$$

Because $-6 \equiv 1 \pmod{7}$ and $-8 \equiv 6 \pmod{7}$, it follows that if x is a solution, then $x \equiv -8 \equiv 6 \pmod{7}$

We need to determine if every x with $x \equiv 6 \pmod{7}$ is a solution. Assume that $x \equiv 6 \pmod{7}$. By Theorem 5 of Section 4.1, it follows that $3x \equiv 3 \cdot 6 = 18 \equiv 4 \pmod{7}$ which shows that all such x satisfy the congruence.

The solutions are the integers x such that $x \equiv 6 \pmod{7}$, namely, 6,13,20 … and $-1, -8, -15, \ldots$

The Chinese Remainder Theorem

Theorem 2: (*The Chinese Remainder Theorem*) Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$.

(That is, there is a solution x with $0 \leq x < m$ and all other solutions are congruent modulo m to this solution.)

- **Proof**: We'll show that a solution exists by describing a way to construct the solution. Showing that the solution is unique modulo m is Exercise 30.

continued →

The Chinese Remainder Theorem

To construct a solution first let $M_k = m/m_k$ for $k = 1,2,\ldots,n$ and $m = m_1 m_2 \cdots m_n$.

Since $\gcd(m_k, M_k) = 1$, by Theorem 1, there is an integer y_k, an inverse of M_k modulo m_k, such that

$$M_k y_k \equiv 1 \pmod{m_k}.$$

Form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n \pmod{m}$$

Note that because $M_j \equiv 0 \pmod{m_k}$ whenever $j \neq k$, all terms except the kth term in this sum are congruent to 0 modulo m_k.

Because $M_k y_k \equiv 1 \pmod{m_k}$, we see that $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$, for $k = 1,2,\ldots,n$.

Hence, x is a simultaneous solution to the n congruences.

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

The Chinese Remainder Theorem

Example: Consider the 3 congruences from Sun-Tsu's problem:

$x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.

- Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_3 = m/5 = 21$, $M_3 = m/7 = 15$.
- We see that
  - 2 is an inverse of $M_1 = 35$ modulo 3 since $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod 3$
  - 1 is an inverse of $M_2 = 21$ modulo 5 since $21 \equiv 1 \pmod 5$
  - 1 is an inverse of $M_3 = 15$ modulo 7 since $15 \equiv 1 \pmod 7$
- Hence,

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod m$$
$$= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}$$

- We have shown that 23 is the smallest positive integer that is a simultaneous solution. Check it!

The Chinese Remainder Theorem

Word Problem:

Jessica breeds rabbits. She's not sure exactly how many she has today, but as she was moving them about this morning, she noticed some things. When she fed them, in groups of 5, she had 4 left over. When she bathed them, in groups of 8, she had a group of 6 left over. She took them outside to romp in groups of 9, but then the last group consisted of only 8. She's positive that there are fewer than 250 rabbits - but how many does she have?

Solution:

We have the following congurences

$x \equiv 4 \pmod 5$,

$x \equiv 6 \pmod 8$,

$x \equiv 8 \pmod 9$.

Cryptography

Section Summary

- Classical Cryptography
- Cryptosystems
- Public Key Cryptography
- RSA Cryptosystem
- Fermat's Little theorem

Caesar Cipher

Julius Caesar created secret messages by shifting each letter three letters forward in the alphabet (sending the last three letters to the first three letters.) For example, the letter B is replaced by E and the letter X is replaced by A. This process of making a message secret is an example of *encryption*.

Here is how the encryption process works:

- Replace each letter by an integer from $\mathbf{Z}_{26}$, that is an integer from 0 to 25 representing one less than its position in the alphabet.
- The encryption function is $f(p) = (p + 3)$ **mod** 26. It replaces each integer p in the set $\{0,1,2,\ldots,25\}$ by $f(p)$ in the set $\{0,1,2,\ldots,25\}$.
- Replace each integer p by the letter with the position $p + 1$ in the alphabet.

Example: Encrypt the message "MEET YOU IN THE PARK" using the Caesar cipher.

Solution: 12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10.

Now replace each of these numbers p by $f(p) = (p + 3)$ **mod** 26.

15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13.

Translating the numbers back to letters produces the encrypted message

"PHHW BRX LQ WKH SDUN."

Caesar Cipher

- To recover the original message, use $f^{-1}(p) = (p-3) \bmod 26$. So, each letter in the coded message is shifted back three letters in the alphabet, with the first three letters sent to the last three letters. This process of recovering the original message from the encrypted message is called *decryption*.
- The Caesar cipher is one of a family of ciphers called *shift ciphers*. Letters can be shifted by an integer k, with 3 being just one possibility. The encryption function is

  $$f(p) = (p + k) \bmod 26$$

  and the decryption function is

  $$f^{-1}(p) = (p-k) \bmod 26$$

  The integer k is called a *key*.

Shift Cipher

Example 1: Encrypt the message "STOP GLOBAL WARMING" using the shift cipher with $k = 11$.

Solution: Replace each letter with the corresponding element of $\mathbf{Z}_{26}$.

18 19 14 15 6 11 14 1 0 11 22 0 17 12 8 13 6.

Apply the shift $f(p) = (p + 11)$ **mod** 26, yielding

3 4 25 0 17 22 25 12 11 22 7 11 2 23 19 24 17.

Translating the numbers back to letters produces the ciphertext

"DEZA RWZMLW HLCXTYR."

Shift Cipher

Example 2: Decrypt the message "LEWLYPLUJL PZ H NYLHA ALHJOLY" that was encrypted using the shift cipher with $k = 7$.

Solution: Replace each letter with the corresponding element of $\mathbf{Z}_{26}$.

11 4 22 11 24 15 11 20 9 11 15 25 7 13 24 11 7 0 0 11 7 9 14 11 24.

Shift each of the numbers by $-k = -7$ modulo 26, yielding

4 23 15 4 17 8 4 13 2 4 8 18 0 6 17 4 0 19 19 4 0 2 7 4 17.

Translating the numbers back to letters produces the decrypted message

"EXPERIENCE IS A GREAT TEACHER."

Number Theory in Cryptography

Terminology: Two parties **Alice** and **Bob** want to communicate securely s.t. a third party **Eve** who intercepts messages cannot learn the content of the messages.

Symmetric Cryptosystems: Alice and Bob share a secret. Only they know a secret key K that is used to encrypt and decrypt messages. Given a message M, Alice encodes it (possibly with padding) into m, and then sends the ciphertext $encrypt(m, K)$ to Bob. Then Bob uses K to decrypt it and obtains $decrypt(encrypt(m, K), K) = m$.
Example: AES.

Public Key Cryptosystems: Alice and Bob do a-priori **not** share a secret. How can they establish a shared secret when others are listening to their messages?

Idea: Have a two-part key, i.e., a key pair. A public key that is used to encrypt messages, and a secret key to decrypt them. Alice uses Bob's public key to encrypt a message (everyone can do that). Only Bob can decrypt the message with his secret key.

Description of RSA: Key generation

- Choose two distinct prime numbers p and q. Numbers p and q should be chosen at random, and be of similar bit-length. Prime integers can be efficiently found using a primality test.
- Let $n = pq$ and $k = (p-1)(q-1)$. (In particular, $k = |Z_n^*|$).
- Choose an integer e such that $1 < e < k$ and $gcd(e, k) = 1$; i.e., e and k are coprime.
  e (for encryption) is released as the public key exponent.
  (e must not be very small.)
- Let d be the multiplicative inverse of e modulo k, i.e., $de \equiv 1 (\mod k)$. (Computed using the extended Euclidean algorithm.) d (for decryption) is the private key and kept secret.

The public key is (n, e) and the private key is (n, d).

RSA: Encryption and Decryption

Alice transmits her public key (n, e) to Bob and keeps the private key secret.

Encryption: Bob then wishes to send message M to Alice. He first turns M into an integer m, such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c corresponding to

$$c \equiv m^e \mod n$$

This can be done quickly using the method of exponentiation by squaring. Bob then transmits c to Alice.

Decryption: Alice can recover m from c by using her private key exponent d via computing

$$m \equiv c^d \mod n$$

Given m, she can recover the original message M by reversing the padding scheme.

Using RSA

Given pubKey = <e, n> and privKey = <d, n>

If Message = m

Then:

encryption: $c = m^e \bmod n$, $m < n$

decryption: $m = c^d \bmod n$

signature: $s = md \bmod n$, $m < n$

verification: $m = se \bmod n$

Example of RSA (1)

Choose p = 7 and q = 17.

Compute n = p*q= 119.

Compute f(n)=(p-1)(q-1)=96.

Select e = 5, (a relatively prime to f(n).)

Compute d = _77_such that e*d=1 mod f(n).

- Public key: <5,119>
- Private key: <77,119>
- Message = 19
- Encryption: 19^5 mod 119 = 66
- Decryption: 66^{77} mod 119 = 19

Example of RSA (2)

p = 7, q = 11, n = 77

Alice chooses e = 17, making d = 53

Bob wants to send Alice secret message

HELLO (07 04 11 11 14)

– 07^{17} mod 77 = 28; 04^{17} mod 77 = 16

– 11^{17} mod 77 = 44; – 11^{17} mod 77 = 44

– 14^{17} mod 77 = 42

- Bob sends 28 16 44 44 42

Example of RSA (3)

Alice receives **28 16 44 44 42**

Alice uses private key, d = 53, to decrypt message:

– 28^{53} mod 77 = 07; 16^{53} mod 77 = 04

– 44^{53} mod 77 = 11; 44^{53} mod 77 = 11

– 42^{53} mod 77 = 14

• Alice translates **07 04 11 11 14** to ***HELLO***

No one else could read it, as only Alice knows her private key (needed for decryption)

Fermat's Little Theorem

Pierre de Fermat
(1601-1665)

Theorem 3: (*Fermat's Little Theorem*) If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$

Furthermore, for every integer a we have $a^p \equiv a \pmod{p}$

(*proof outlined in Exercise 19*)

Fermat's little theorem is useful in computing the remainders modulo p of large powers of integers.

Example: Find 7^{222} **mod** 11.

By Fermat's little theorem, we know that $7^{10} \equiv 1 \pmod{11}$, and so $(7^{10})^k \equiv 1 \pmod{11}$, for every positive integer k. Therefore,

$$7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} 7^2 \equiv (1)^{22} \cdot 49 \equiv 5 \pmod{11}.$$

Hence, 7^{222} **mod** $11 = 5$.

The Foundations: Logic and Proofs

Proofs

- A proof is a valid argument that establishes the truth of a mathematical statement.

- Ingredients:
  - hypotheses of the theorem
  - axioms assumed to be true
  - previously proven theorems
  - rules of inference

You get: truth of the statement being proved

Usefulness

- Computer Science
  - Verifying that computer programs are correct.
  - Establishing that operating systems are secure.
  - Making inferences in artificial intelligence.
  - Showing that system specifications are consistent.

- Mathematics
  - Defining Formalism.
  - Providing specification in a common language.
  - Justification for the results.

Definitions

1. An integer n is even if, and only if, n = 2k for some integer k.

2. An integer n is odd if, and only if, n = 2k + 1 for some integer k.

3. An integer n is prime if, and only if, n > 1 and for all positive integers r and s, if n = r·s, then r = 1 or s = 1.

4. An integer n > 1 is composite if, and only if, n = r·s for some positive integers r and s with r ≠ 1 and s ≠ 1.

5. A real number r is rational if, and only if, r= $\frac{a}{b}$ for some integers a and b with b ≠ 0.

6. If n and d are integers and d ≠ 0, then d divides n, written d|n if, and only if, n = d.k for some integers k.

7. An integer n is called a perfect square if, and only if, n = k^2 for some integer k.

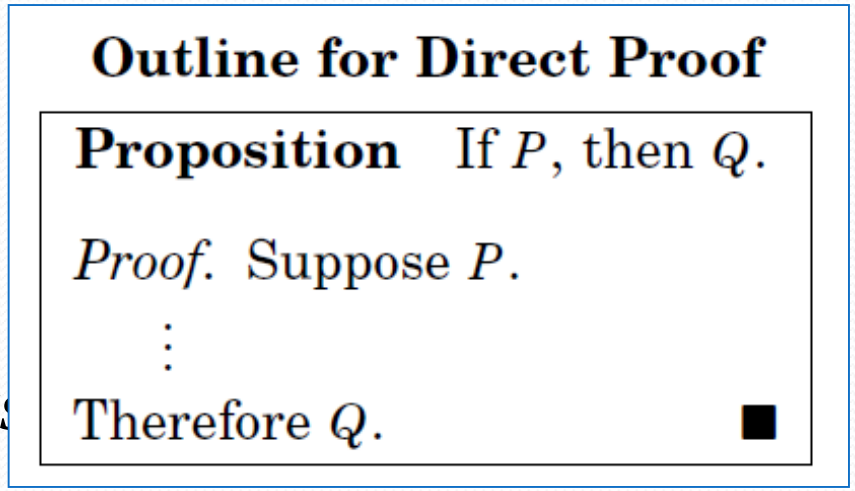
Types of Proofs

- **Proving conditional Statements**
  - Direct Proofs
  - Indirect Proofs
    - **Proof by Contraposition**
    - **Proofs by Contradiction**
- **Proving Non-conditional Statements**
  - Indirect Proofs
  - If-And-Only-If Proof
  - Constructive Versus Non-constructive Proofs
  - Existence Proofs; Existence and Uniqueness Proofs
  - Disproofs (Counterexample, Contradiction, Existence Statement)
  - Proofs Involving Sets
- **Mathematical Induction**

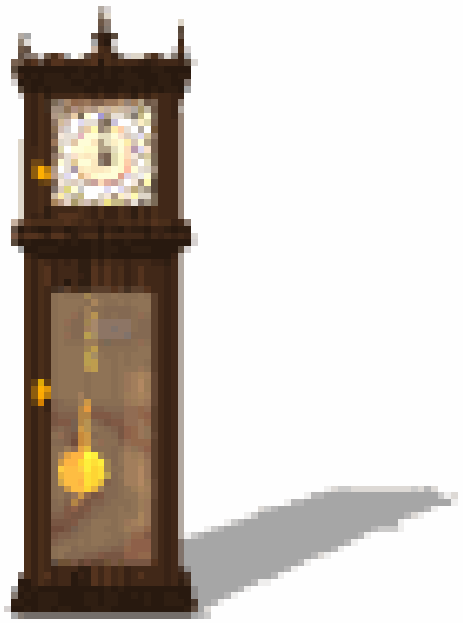
Direct Proofs

- p →q
  - first step is the assumption that *p is true*
  - subsequent steps constructed using rules of inference.
  - final step showing that *q must also be true*

showing that if *p is true,*
then q must also be true,
so that the combination
p true and q false never occurs



Activity Time



Prove that the sum of two odd integers is even.

Prove that the sum of two odd integers is even.

Let **m** and **n** be two odd integers. Then by definition of odd numbers

$m = 2k + 1$ for some $k \in Z$

$n = 2l + 1$ for some $l \in Z$

Now $m + n = (2k + 1) + (2l + 1)$

$= 2k + 2l + 2$

$= 2(k + l + 1)$

$= 2r$ where $r = (k + l + 1) \in Z$

Hence $m + n$ is even.

EXERCISE:

Prove that if n is any even integer, then $(-1)^n = 1$

SOLUTION:

Suppose n is an even integer. Then $n = 2k$ for some integer k.

Now

$$(-1)^n = (-1)^{2k}$$
$$= [(-1)^2]^k$$
$$= (1)^k$$
$$= 1 \qquad \text{(proved)}$$

EXERCISE:

Prove that the product of an even integer and an odd integer is even.

SOLUTION:

Suppose m is an even integer and n is an odd integer. Then

$m = 2k$ for some integer k

and $n = 2l + 1$ for some integer l

Now

$$m \cdot n = 2k \cdot (2l + 1)$$
$$= 2 \cdot k\,(2l + 1)$$
$$= 2 \cdot r \quad \text{where } r = k(2l + 1) \text{ is an integer}$$

Hence $m \cdot n$ is even. (Proved)

EXERCISE:

Prove that the square of an even integer is even.

SOLUTION:

Suppose n is an even integer. Then $n = 2k$

Now

$$\text{square of } n = n^2 = (2 \cdot k)^2$$
$$= 4k^2$$
$$= 2 \cdot (2k^2)$$
$$= 2 \cdot p \text{ where } p = 2k^2 \in Z$$

Hence, n^2 is even. (proved)

proved that if *n is an odd integer, then n^2 is an odd integer*

- We assume that the hypothesis of this conditional statement is true, namely, we assume that *n is odd.*
- By the definition of an odd integer, it follows that $n = 2k + 1$, *where k is some integer.*
- *Square both sides* $n^2 = (2k + 1)^2$
  - $4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.
- Consequently, we have proved that if *n is an odd integer, then* n^2 *is an odd integer*

EXERCISE:

Prove that if n is an odd integer, then $n^3 + n$ is even.

SOLUTION:

Let n be an odd integer, then $n = 2k + 1$ for some $k \in Z$

Now $n^3 + n = n(n^2 + 1)$

$= (2k + 1)((2k+1)^2 + 1)$

$= (2k + 1)(4k^2 + 4k + 1 + 1)$

$= (2k + 1)(4k^2 + 4k + 2)$

$= (2k + 1)\,2.(2k^2 + 2k + 1)$

$= 2\cdot(2k + 1)(2k^2 + 2k + 1)$ $\quad k \in Z$

= an even integer

Proposition If x is an even integer, then $x^2 - 6x + 5$ is odd.

Proof. Suppose x is an even integer.

Then $x = 2a$ for some $a \in \mathbb{Z}$, by definition of an even integer.

So $x^2 - 6x + 5 = (2a)^2 - 6(2a) + 5 = 4a^2 - 12a + 5 = 4a^2 - 12a + 4 + 1 = 2(2a^2 - 6a + 2) + 1$.

Therefore we have $x^2 - 6x + 5 = 2b + 1$, where $b = 2a^2 - 6a + 2 \in \mathbb{Z}$.

Consequently $x^2 - 6x + 5$ is odd, by definition of an odd number.

EXERCISE:

Prove that, if the sum of any two integers is even, then so is their difference.

SOLUTION:

Suppose m and n are integers so that m + n is even. Then by definition of even numbers

$m + n = 2k$ for some integer k

$\Rightarrow \quad m = 2k - n$ .....(1)

Now $m - n = (2k - n) - n$ using (1)

$= 2k - 2n$

$= 2(k - n) = 2r$ where $r = k - n$ is an integer

Hence m - n is even.

EXERCISE:

Prove that the sum of any two rational numbers is rational.

SOLUTION:

Suppose r and s are rational numbers.

Then by definition of rational

$$r = \frac{a}{b} \quad \text{and} \quad s = \frac{c}{d}$$

for some integers a, b, c, d with $b \neq 0$ and $d \neq 0$

Now

$$r + s = \frac{a}{b} + \frac{c}{d}$$

$$= \frac{ad + bc}{bd}$$

$$= \frac{p}{q}$$

where $p = ad + bc \in Z$ and $q = bd \in Z$ and $q \neq 0$

Hence r + s is rational.

EXERCISE:

Given any two distinct rational numbers r and s with $r < s$. Prove that there is a rational number x such that $r < x < s$.

SOLUTION:

Given two distinct rational numbers r and s such that

$r < s$ .....(1)

Adding r to both sides of (1), we get

$$r + r < r + s$$

$$2r < r + s$$

$$\Rightarrow \quad r < \frac{r+s}{2} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

Next adding s to both sides of (1), we get

$$r + s < s + s$$

$$\Rightarrow \quad r + s < 2s$$

$$\Rightarrow \quad \frac{r+s}{2} < s \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

Combining (2) and (3), we may write

$$r < \frac{r+s}{2} < s \qquad \text{.....(4)}$$

Since the sum of two rationals is rational, therefore $r + s$ is rational. Also the quotient of a rational by a non-zero rational, is rational, therefore $\frac{r+s}{2}$ is rational and by (4) it lies between r & s. Hence, we have found a rational number such that $r < x < s$. (proved)

EXERCISE:

Prove that the sum of any three consecutive integers is divisible by 3.

PROOF:

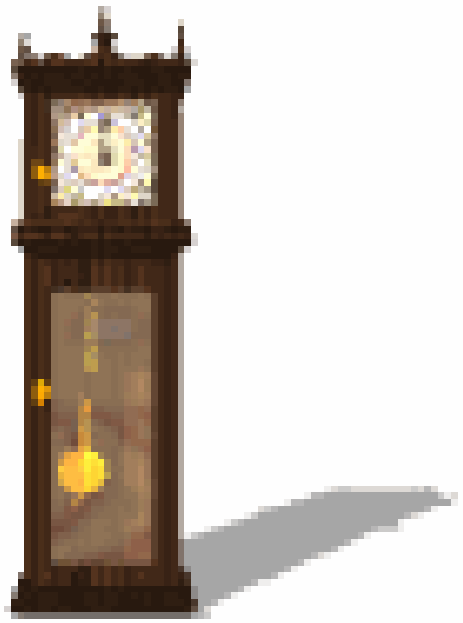
Let n, $n + 1$ and $n + 2$ be three consecutive integers.

Now

$$n + (n + 1) + (n + 2) = 3n + 3$$
$$= 3(n + 1)$$
$$= 3 \cdot k \quad \text{where } k = (n+1) \in Z$$

Hence, the sum of three consecutive integers is divisible by 3.

Activity Time

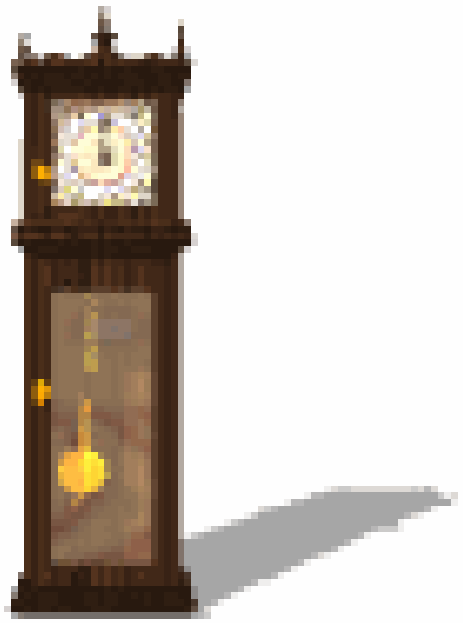


Give a direct proof that if *m and n are both perfect squares, then nm is also a perfect square.*

Proof

- We assume that the hypothesis of this conditional statement is true, namely, we assume that m and n are both perfect squares.
- By the definition of a perfect square, It follows that there are integers s and t such that $m = s^2$ and $n = t^2$.
- Multiplying both m and n to get s^2t^2.
- Hence, $mn = s^2t^2 = (ss)(tt) = (st)(st) = (st)^2$, using commutativity and associativity of multiplication.
- By the definition of perfect square, it follows that mn is also a perfect square, because it is the square of st, which is an integer.
- We have proved that if m and n are both perfect squares, then mn is also a perfect square.

Activity Time



Give a direct proof that if *n is an integer and n is odd, then 3n + 2 is odd.*

Indirect Proofs

- Direct proof begin with the premises, continue with a sequence of deductions, and end with the conclusion.
- Attempts at direct proofs often reach dead ends
- Proofs that **do not** start with the premises and end with the conclusion, are called **indirect proofs**

PROOF BY CONTRAPOSITION:

A proof by contraposition is based on the logical equivalence between a statement and its contrapositive. Therefore, the implication $p \rightarrow q$ can be proved by showing that its contrapositive $\sim q \rightarrow \sim p$ is true. The contrapositive is usually proved directly.

The method of proof by contrapositive may be summarized as:

1. Express the statement in the form if p then q.
2. Rewrite this statement in the contrapositive form
   if not q then not p.
3. Prove the contrapositive by a direct proof.

Outline for Contrapositive Proof

Proposition If P, then Q.

Proof. Suppose $\sim Q$.

⋮

Therefore $\sim P$. ■

Prove that if *n is an integer and 3n + 2 is odd, then n is odd.*

PROOF:

The contrapositive of the given conditional statement is

" if n is even then 3n + 2 is even"

Suppose n is even, then

$n = 2k$ for some $k \in Z$

Now $3n + 2 = 3(2k) + 2$

$= 2.(3k + 1)$

$= 2.r$ where $r = (3k + 1) \in Z$

Hence 3n + 2 is even. We conclude that the given statement is true since its contrapositive is true.

EXERCISE:

Prove that for all integers n, if n^2 is even then n is even.

PROOF:

The contrapositive of the given statement is:

"if n is not even (odd) then n^2 is not even (odd)"

We prove this contrapositive statement directly.

Suppose n is odd. Then $n = 2k + 1$ for some $k \in Z$

Now $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$

$= 2 \cdot (2k^2 + 2k) + 1$

$= 2 \cdot r + 1$ where $r = 2k^2 + 2k \in Z$

Hence n^2 is odd. Thus the contrapositive statement is true and so the given statement is true.

EXERCISE:

Prove that if n is an integer and $n^3 + 5$ is odd, then n is even.

PROOF:

Suppose n is an odd integer. Since, a product of two odd integers is odd, therefore n^2 = n.n is odd; and $n^3 = n^2.n$ is odd.

Since a sum of two odd integers is even therefore $n^2 + 5$ is even.

Thus we have prove that if n is odd then $n^3 + 5$ is even.

Since this is the contrapositive of the given conditional statement, so the given statement is true.

EXERCISE:

Prove that if n^2 is not divisible by 25, then n is not divisible by 5.

SOLUTION:

The contra positive statement is:

"if n is divisible by 5, then n^2 is divisible by 25"

Suppose n is divisible by 5. Then by definition of divisibility

$$n = 5 \cdot k \qquad \text{for some integer } k$$

Squaring both sides

$$n^2 = 25 \cdot k^2 \qquad \text{where } k^2 \in Z$$

n^2 is divisible by 25

Proofs by Contradiction

A proof by contradiction is based on the fact that either a statement is true or it is false but not both. Hence the supposition, that the statement to be proved is false, leads logically to a contradiction, impossibility or absurdity, then the supposition must be false. Accordingly, the given statement must be true.

The method of proof by contradiction may be summarized as follows:

1. Suppose the statement to be proved is false.

2. Show that this supposition leads logically to a contradiction.

3. Conclude that the statement to be proved is true.

Basic Idea

- Assume that the statement we want to prove is *false, and then show* that this assumption leads to nonsense!

Outline for Proof by Contradiction

Proposition P.

Proof. Suppose $\sim P$.

⋮

Therefore $C \wedge \sim C$. ■

We are then led to conclude that we were wrong to assume the statement was false, so the statement must be true.

THEOREM:

There is no greatest integer.

PROOF:

Suppose there is a greatest integer N. Then $n \leq N$ for every integer n.

Let $M = N + 1$

Now M is an integer since it is a sum of integers.

Also $M > N$ since $M = N + 1$

Thus M is an integer that is greater than the greatest integer, which is a contradiction. Hence our supposition is not true and so there is no greatest integer.

EXERCISE:

Give a proof by contradiction for the statement:

"If n^2 is an even integer then n is an even integer."

PROOF:

Suppose n^2 is an even integer and n is not even, so that n is odd.

Hence $n = 2k + 1$ for some integer k.

Now $n^2 = (2k + 1)^2$

$= 4k^2 + 4k + 1$

$= 2 \cdot (2k^2 + 2k) + 1$

$= 2r + 1$ where $r = (2k^2 + 2k) \in Z$

This shows that n^2 is odd, which is a contradiction to our supposition that n^2 is even. Hence the given statement is true.

EXERCISE:

Prove that if n is an integer and $n^3 + 5$ is odd, then n is even using contradiction method.

SOLUTION:

Suppose that $n^3 + 5$ is odd and n is not even (odd). Since n is odd and the product of two odd numbers is odd, it follows that n^2 is odd and $n^3 = n^2 . n$ is odd. Further, since the difference of two odd numbers is even, it follows that

$$5 = (n^3 + 5) - n^3$$

is even. But this is a contradiction. Therefore, the supposition that $n^3 + 5$ and n are both odd is wrong and so the given statement is true.

THEOREM:

The sum of any rational number and any irrational number is irrational.

PROOF:

We suppose that the negation of the statement is true. That is, we suppose that there is a rational number r and an irrational number s such that r + s is rational. By definition of ration

$$r = \frac{a}{b} \quad \ldots\ldots\ldots\ldots\ldots(1) \quad \text{and} \quad r + s = \frac{c}{d} \quad \ldots\ldots\ldots\ldots\ldots(2)$$

for some integers a, b, c and d with b$\neq$ 0 and d $\neq$ 0.

Using (1) in (2), we get

$$\frac{a}{b} + s = \frac{c}{d}$$

$$\Rightarrow \quad s = \frac{c}{d} - \frac{a}{b}$$

$$s = \frac{bc - ad}{bd} \qquad (bd \neq 0)$$

Now bc - ad and bd are both integers, since products and difference of integers are integers. Hence s is a quotient of two integers bc-ad and bd with bd $\neq$ 0. So by definition of rational, s is rational.

This contradicts the supposition that s is irrational. Hence the supposition is false and the theorem is true.

EXERCISE:

Prove that $\sqrt{2}$ is irrational.

PROOF:

Suppose $\sqrt{2}$ is rational. Then there are integers m and n with no common factors so

$$\sqrt{2} = \frac{m}{n}$$

that

Squaring both sides gives

$$2 = \frac{m^2}{n^2}$$

Or $m^2 = 2n^2$ .....(1)

This implies that m^2 is even (by definition of even). It follows that m is even. Hence

$m = 2k$ for some integer k (2)

Substituting (2) in (1), we get

$$(2k)^2 = 2n^2$$

$$\Rightarrow \quad 4k^2 = 2n^2$$

$$\Rightarrow \quad n^2 = 2k^2$$

This implies that n^2 is even, and so n is even. But we also know that m is even. Hence both m and n have a common factor 2. But this contradicts the supposition that m and n have no common factors. Hence our supposition is false and so the theorem is true.

PROOF BY COUNTER EXAMPLE

Disprove the statement by giving a counter example.
For all real numbers a and b, if $a < b$ then $a^2 < b^2$.

SOLUTION:

Suppose $a = -5$ and $b = -2$
then clearly $-5 < -2$

But $a^2 = (-5)^2 = 25$ and $b^2 = (-2)^2 = 4$

But $25 > 4$

This disproves the given statement.

EXERCISE:

Prove or give counter example to disprove the statement.

For all integers n, $n^2 - n + 11$ is a prime number.

SOLUTION:

The statement is not true

For n = 11

we have , $n^2 - n + 11 = (11)^2 - 11 + 11$

$= (11)^2$

$= (11)(11)$

$= 121$

which is obviously not a prime number.

Mathematical Induction

Shoaib Raza

Conjecture: The sum of the first n odd natural numbers equals n^2.

n	sum of the first n odd natural numbers	n^2
1	$1 = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$	1
2	$1+3 = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$	4
3	$1+3+5 = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$	9
4	$1+3+5+7 = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$	16
5	$1+3+5+7+9 = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$	25
⋮	⋮	⋮
n	$1+3+5+7+9+11+\cdots+(2n-1) = \ldots\ldots\ldots$	n^2
⋮	⋮	⋮

An infinite ladder

- Suppose that we have an infinite ladder, and we want to know whether we can reach every step on this ladder.

- We know two things:
  1. We can reach the first rung of the ladder.
  2. If we can reach a particular rung of the ladder, then we can reach the next rung.

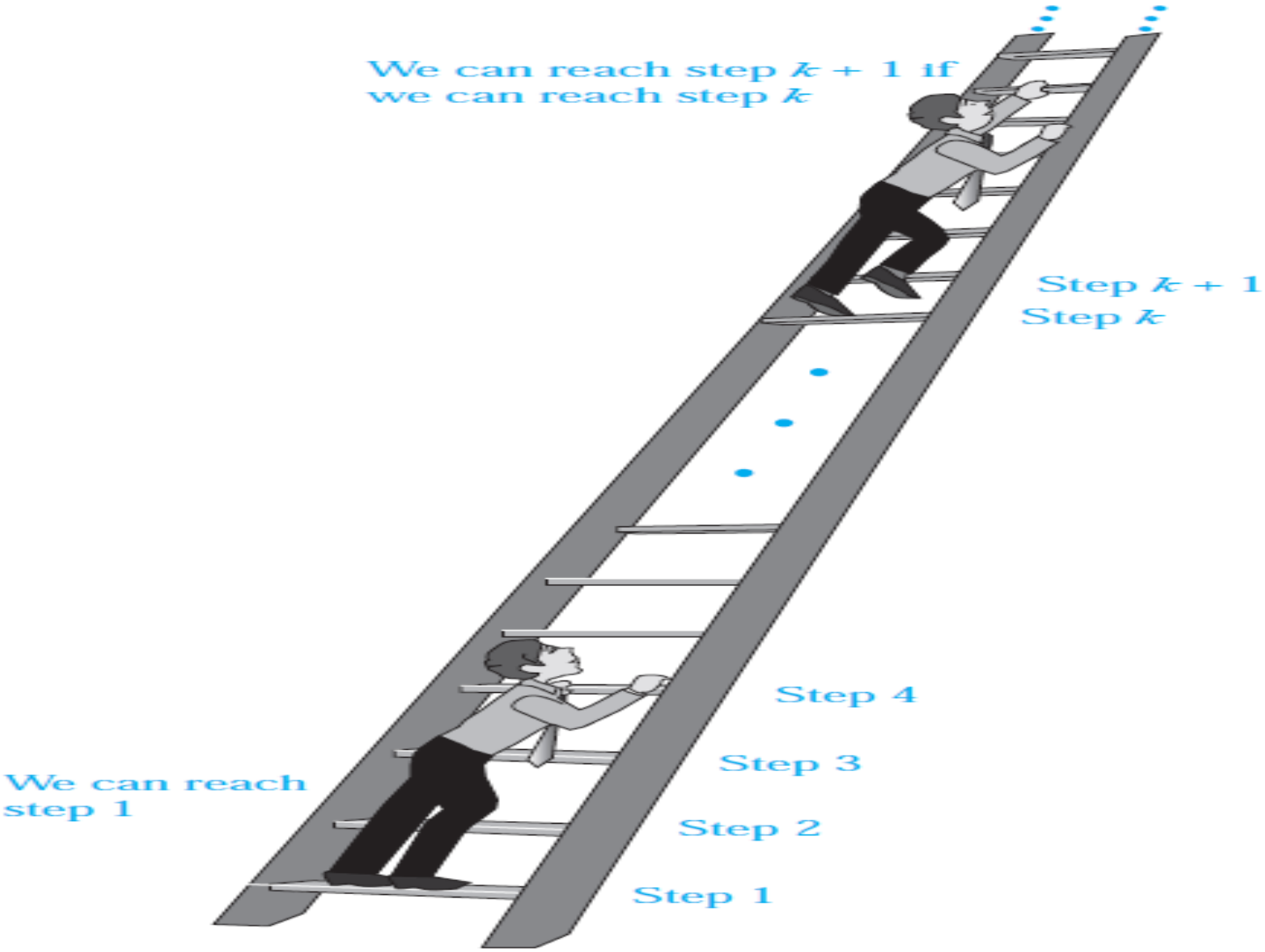


FIGURE 1 **Climbing an Infinite Ladder.**

Mathematical Induction

- Mathematical statements assert that a property is true for all positive integers.

- Proofs using mathematical induction have two parts.
  - First, they show that the statement holds for the positive integer 1 (base case).
  - Second, they show that if the statement holds for a positive integer then it must also hold for the next larger integer. (inductive case)

- The method can be extended to prove statements about more general well-founded structures, such as trees; this generalization, known as structural induction, is used in mathematical logic and computer science.

NOTE

- It is extremely important to note that mathematical induction can be used only to prove results obtained in some other way.
- It is *not a tool for discovering formulae or* theorems.
- Mathematicians sometimes find proofs by mathematical induction unsatisfying because they do not provide insights as to why theorems are true.
- You can prove a theorem by mathematical induction even if you do not have the slightest idea why it is true!

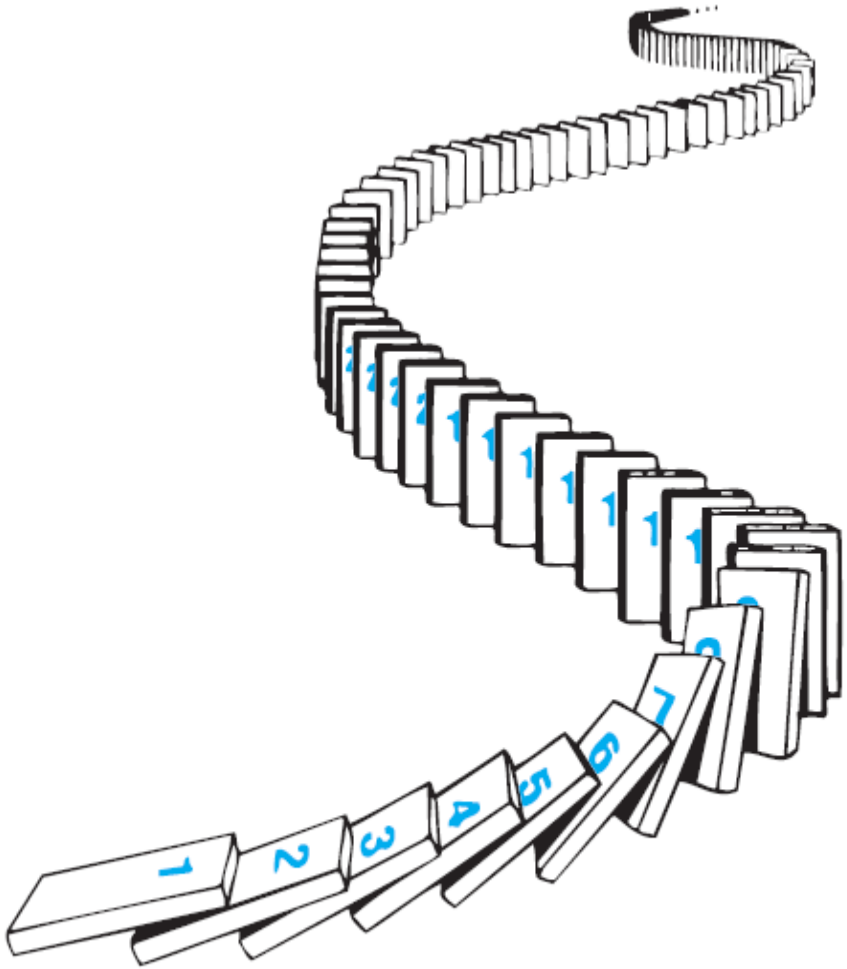
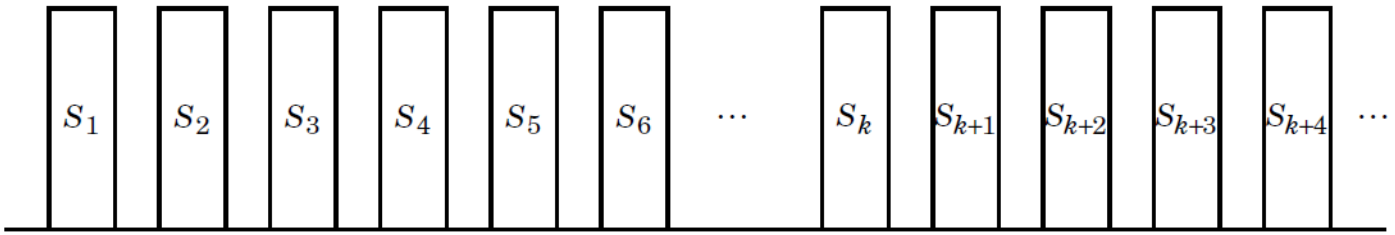
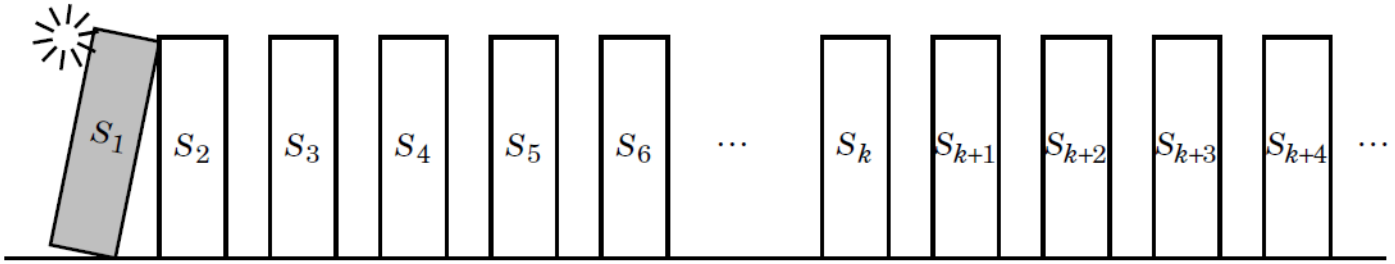


FIGURE 2 Illustrating How Mathematical Induction Works Using Dominoes.

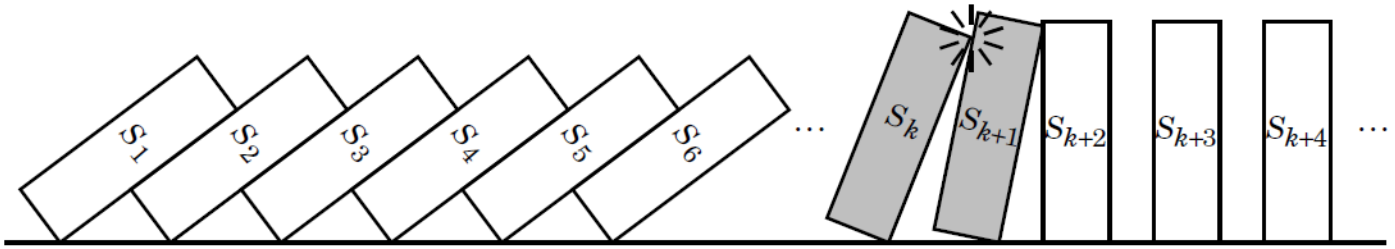
The Simple Idea Behind Mathematical Induction



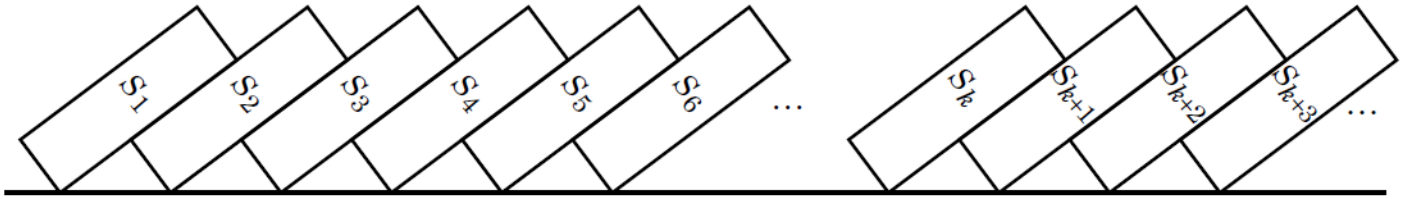
Statements are lined up like dominoes.



(1) Suppose the first statement falls (i.e. is proved true);



(2) Suppose the k^{th} falling always causes the $(k+1)^{th}$ to fall;



Then all must fall (i.e. all statements are proved true).

PRINCIPLE OF MATHEMATICAL INDUCTION:

Let P(n) be a propositional function defined for all positive integers n. P(n) is true for every positive integer n if

1.Basis Step:

The proposition P(1) is true.

2.Inductive Step:

If P(k) is true then P(k + 1) is true for all integers $k \geq 1$.

i.e. $\forall k \quad p(k) \rightarrow P(k+1)$

EXAMPLE:

Use Mathematical Induction to prove that

$$1+2+3+\cdots+n=\frac{n(n+1)}{2} \quad \text{for all integers } n \geq 1$$

SOLUTION:

Let $$P(n):1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

1.Basis Step:

P(1) is true.

For n = 1, left hand side of P(1) is the sum of all the successive integers starting at 1 and ending at 1, so LHS = 1 and RHS is

$$R.H.S=\frac{1(1+1)}{2}=\frac{2}{2}=1$$

so the proposition is true for n = 1.

2. Inductive Step: Suppose P(k) is true for, some integers $k \geq 1$.

(1) $$1+2+3+\cdots+k=\frac{k(k+1)}{2}$$

To prove P(k + 1) is true. That is,

$$(2) \qquad 1+2+3+\cdots+(k+1)=\frac{(k+1)(k+2)}{2}$$

Consider L.H.S. of (2)

$$1+2+3+\cdots+(k+1) = 1+2+3+\cdots+k+(k+1)$$

$$= \frac{k(k+1)}{2}+(k+1) \qquad \text{using (1)}$$

$$= (k+1)\left[\frac{k}{2}+1\right]$$

$$= (k+1)\left[\frac{k+2}{2}\right]$$

$$= \frac{(k+1)(k+2)}{2} = \text{RHS of (2)}$$

Hence by principle of Mathematical Induction the given result true for all integers greater or equal to 1.

EXERCISE:

Use mathematical induction to prove that
$1+3+5+\ldots+(2n-1) = n^2$ for all integers $n \geq 1$.

SOLUTION:

Let P(n) be the equation $1+3+5+\ldots+(2n-1) = n^2$

1. **Basis Step:**

   P(1) is true
   For n = 1, L.H.S of P(1) = 1and
   R.H.S = $1^2 = 1$
   Hence the equation is true for n = 1

2. **Inductive Step:**

   Suppose P(k) is true for some integer $k \geq 1$. That is,
   $1 + 3 + 5 + \ldots + (2k - 1) = k^2$ .....(1)

To prove P(k+1) is true; i.e.,
$1 + 3 + 5 + \ldots + [2(k+1)-1] = (k+1)^2$ .....(2)

Consider L.H.S. of (2)

$$1+3+5+\cdots+[2(k+1)-1] = 1+3+5+\cdots+(2k+1)$$
$$= 1+3+5+\cdots+(2k-1)+(2k+1)$$
$$= k^2+(2k+1) \quad \text{using (1)}$$
$$= (k+1)^2$$
$$= \text{R.H.S. of (2)}$$

Thus P(k+1) is also true. Hence by mathematical induction, the given equation is true for all integers $n \geq 1$.

Exercise (cont.)

Proof.

1. $P(n)$: $2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$
2. Basis step $P(0)$: $2^0 = 1 = 2^{0+1} - 1$.
3. Inductive step:
   Inductive hypothesis $P(k)$: $2^0 + 2^1 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$
   Let's prove $P(k+1)$:

$$\begin{aligned} 2^0 + 2^1 + 2^2 + \cdots + 2^k + 2^{k+1} &= 2^{k+1} - 1 + 2^{k+1} && \text{(by IH)} \\ &= 2(2^{k+1}) - 1 && \text{(by arithmetic)} \\ &= 2^{k+2} - 1 && \text{(by arithmetic)} \end{aligned}$$