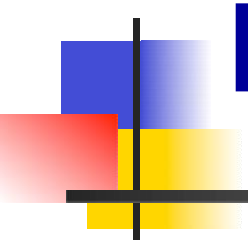


Lecture 9

Chapter 2. Basic Structures

2.2 Set Operations

Set Identities

- Identity: $A \cup \varnothing = A = A \cap U$
- Domination: $A \cup U = U$, $A \cap \varnothing = \varnothing$
- Idempotent: $A \cup A = A$, $A \cap A = A$
- Double complement: $(\overline{A}) = A$
- Commutative: $A \cup B = B \cup A$, $A \cap B = B \cap A$
- Associative: $A \cup (B \cup C) = (A \cup B) \cup C$,
  $A \cap (B \cap C) = (A \cap B) \cap C$
- Distributive: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- Absorption: $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$
- Complement: $A \cup \overline{A} = U$, $A \cap \overline{A} = \varnothing$

DeMorgan's Law for Sets

- Exactly analogous to (and provable from) DeMorgan's Law for propositions.

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

Proving Set Identities

- To prove statements about sets, of the form $E_1 = E_2$ (where the Es are set expressions), here are three useful techniques:

  1. Prove $E_1 \subseteq E_2$ and $E_2 \subseteq E_1$ separately.

  2. Use set builder notation & logical equivalences.

  3. Use a *membership table*.

  4. Use a Venn diagram.

Method 1: Mutual Subsets

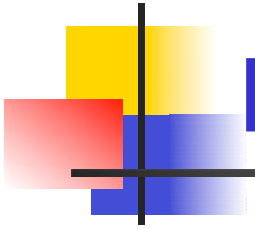
Example: Show $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

- Part 1: Show $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.
  - Assume $x \in A \cap (B \cup C)$, & show $x \in (A \cap B) \cup (A \cap C)$.
  - We know that $x \in A$, and either $x \in B$ or $x \in C$.
    - Case 1: $x \in A$ and $x \in B$. Then $x \in A \cap B$, so $x \in (A \cap B) \cup (A \cap C)$.
    - Case 2: $x \in A$ and $x \in C$. Then $x \in A \cap C$, so $x \in (A \cap B) \cup (A \cap C)$.
  - Therefore, $x \in (A \cap B) \cup (A \cap C)$.
  - Therefore, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.
- Part 2: Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. (Try it!)

Method 2: Set BuilderNotation & Logical Equivalence

- Show $\overline{A \cap B} = \overline{A} \cup \overline{B}$

$\overline{A \cap B} = \{x \mid x \notin (A \cap B)\}$	def. of complement
$= \{x \mid \neg(x \in (A \cap B))\}$	def. of "does not belong"
$= \{x \mid \neg(x \in A \wedge x \in B)\}$	def. of intersection
$= \{x \mid \neg(x \in A) \vee \neg(x \in B)\}$	De Morgan's law (logic)
$= \{x \mid x \notin A \vee x \notin B\}$	def. of "does not belong"
$= \{x \mid x \in \overline{A} \vee x \in \overline{B}\}$	def. of complement
$= \{x \mid x \in \overline{A} \cup \overline{B}\}$	def. of union
$= \overline{A} \cup \overline{B}$	by set builder notation



Method 3: Membership Tables

- Analog to truth tables in propositional logic.
- Columns for different set expressions.
- Rows for all combinations of memberships in constituent sets.
- Use “1” to indicate membership in the derived set, “0” for non-membership.
- Prove equivalence with identical columns.

Membership Table Example

- Prove $(A \cup B) - B = A - B$.

A	B	$A \cup B$	$(A \cup B) - B$	$A - B$
1	1	1	0	0
1	0	1	1	1
0	1	1	0	0
0	0	0	0	0

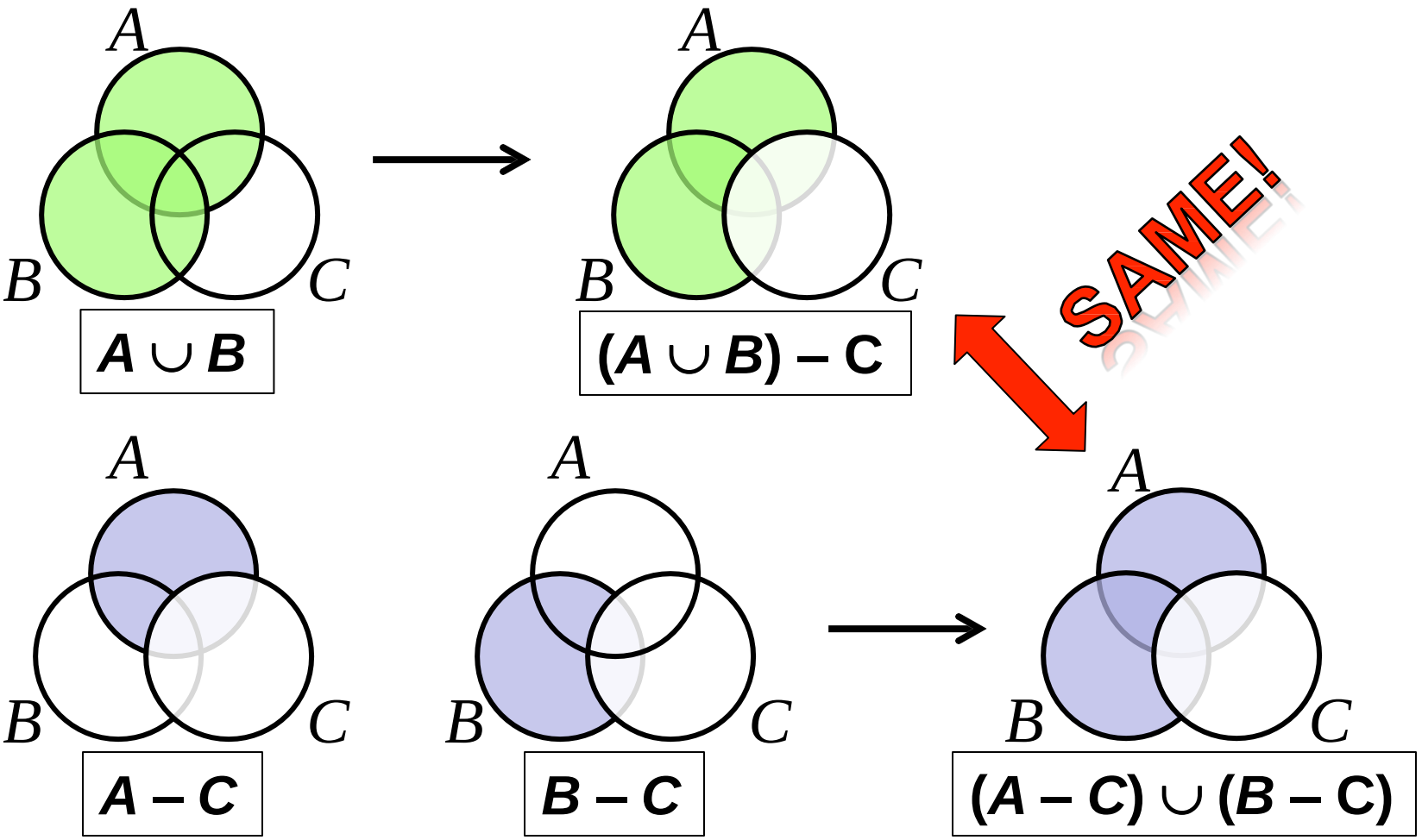
Membership Table Exercise

- Prove $(A \cup B) - C = (A - C) \cup (B - C)$.

A	B	C	$A \cup B$	$(A \cup B) - C$	$A - C$	$B - C$	$(A - C) \cup (B - C)$
1	1	1	1	0	0	0	0
1	1	0	1	1	1	1	1
1	0	1	1	0	0	0	0
1	0	0	1	1	1	0	1
0	1	1	1	0	0	0	0
0	1	0	1	1	0	1	1
0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0

Method 4: Venn Diagram

- Prove $(A \cup B) - C = (A - C) \cup (B - C)$.



Generalized Unions & Intersections

- Since union & intersection are commutative and associative, we can extend them from operating on pairs of sets A and B to operating on sequences of sets $A_1,\ldots, A_n$, or even on sets of sets, $X = \{A \mid P(A)\}$.

Generalized Union

- Binary union operator: $A \cup B$
- *n*-ary union:
  $A_1 \cup A_2 \cup \ldots \cup A_n = ((\ldots((A_1 \cup A_2) \cup \ldots) \cup A_n)$
  (grouping & order is irrelevant)
- "Big U" notation: $\bigcup_{i=1}^{n} A_i$
- More generally, union of the sets A_i for $i \in I$:
  $\bigcup_{i \in I} A_i$
- For infinite number of sets: $\bigcup_{i=1}^{\infty} A_i$

Generalized Union Examples

- Let $A_i = \{i, i+1, i+2, \ldots\}$. Then,

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n$$

$$= \{1,2,3,\ldots\} \cup \{2,3,4,\ldots\} \cup \cdots \cup \{n, n+1, n+2,\ldots\}$$

$$= \{1,2,3,\ldots\}$$

- Let $A_i = \{1, 2, 3, \ldots, i\}$ for $i = 1, 2, 3, \ldots$. Then,

$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup A_3 \cup \cdots$$

$$= \{1\} \cup \{1,2\} \cup \{1,2,3\} \cup \cdots$$

$$= \{1,2,3,\ldots\} = Z^+$$

Generalized Intersection

- Binary intersection operator: $A \cap B$
- n-ary intersection:
  $A_1 \cap A_2 \cap \ldots \cap A_n \equiv ((\ldots((A_1 \cap A_2) \cap \ldots) \cap A_n)$
  (grouping & order is irrelevant)
- "Big Arch" notation: $\bigcap_{i=1}^{n} A_i$
- Generally, intersection of sets A_i for $i \in I$: $\bigcap_{i \in I} A_i$
- For infinite number of sets: $\bigcap_{i=1}^{\infty} A_i$

Generalized Intersection Example

Let $A_i = \{i, i+1, i+2, \ldots\}$. Then,

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n$$

$$= \{1,2,3,\ldots\} \cap \{2,3,4,\ldots\} \cap \cdots \cap \{n, n+1, n+2, \ldots\}$$

$$= \{n, n+1, n+2, \ldots\}$$

- Let $A_i = \{1, 2, 3, \ldots, i\}$ for $i = 1, 2, 3, \ldots$. Then,

$$\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap A_3 \cap \cdots$$

$$= \{1\} \cap \{1,2\} \cap \{1,2,3\} \cap \cdots$$

$$= \{1\}$$

Bit String Representation of Sets

- A frequent theme of this course are methods of *representing* one discrete structure using another discrete structure of a different type.
- For an enumerable universal set U with ordering $x_1, x_2, x_3, \ldots$, we can represent a finite set $S \subseteq U$ as the finite bit string $B = b_1 b_2 \ldots b_n$ where $b_i = 1$ if $x_i \in S$ and $b_i = 0$ if $x_i \notin S$.
- *E.g.* $U = \mathbf{N}$, $S = \{2,3,5,7,11\}$, B = 0011 0101 0001.
- In this representation, the set operators "$\cup$", "$\cap$", "$\overline{}$" are implemented directly by bitwise OR, AND, NOT!

Examples of Sets as Bit Strings

- Let $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, and the ordering of elements of U has the elements in increasing order, then

  $S_1 = \{1, 2, 3, 4, 5\} \Rightarrow B_1 = 11\ 1110\ 0000$

  $S_2 = \{1, 3, 5, 7, 9\} \Rightarrow B_2 = 10\ 1010\ 1010$

  - $S_1 \cup S_2 = \{1, 2, 3, 4, 5, 7, 9\}$

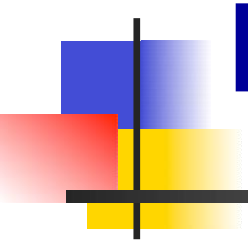
    $\Rightarrow$ bit string = 11 1110 1010 = $\boldsymbol{B_1 \vee B_2}$

  - $S_1 \cap S_2 = \{1, 3, 5\}$

    $\Rightarrow$ bit string = 10 1010 0000 = $\boldsymbol{B_1 \wedge B_2}$

  - $\overline{S_1} = \{6, 7, 8, 9, 10\}$

    $\Rightarrow$ bit string = 00 0001 1111 = $\boldsymbol{\neg B_1}$



Lecture 10

Chapter 2. Basic Structures

2.3 Functions

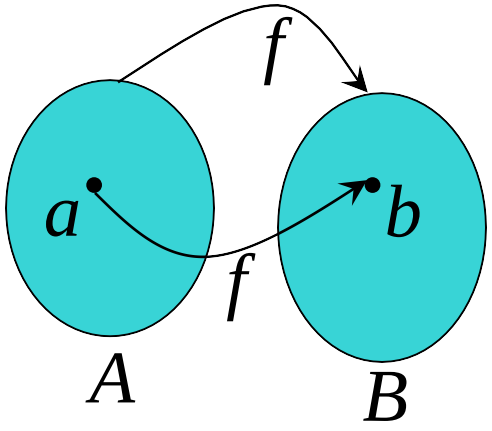
2.3 Functions

- From calculus, you are familiar with the concept of a real-valued function f, which assigns to each number $x \in \mathbf{R}$ a value $y = f(x)$, where $y \in \mathbf{R}$.

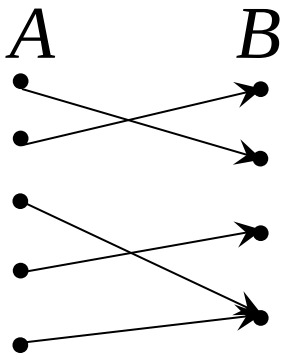
- But, the notion of a function can also be naturally generalized to the concept of assigning elements of *any* set to elements of *any* set. (Also known as a *map*.)

Function: Formal Definition

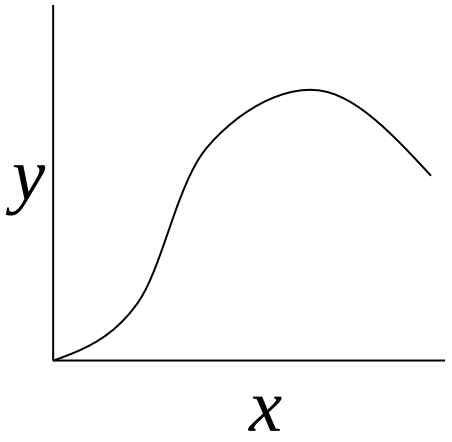
- For any sets A and B, we say that a ***function (or "mapping") f from A to B ($f : A \to B$)*** is a particular assignment of **exactly one element** $f(x) \in B$ to **each element** $x \in A$.
- Functions can be represented graphically in several ways:



Like Venn diagrams



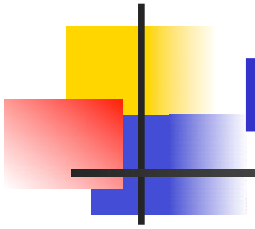
Bipartite Graph



Plot

Some Function Terminology

- If it is written that $f : A \rightarrow B$, and $f(a) = b$ (where $a \in A$ and $b \in B$), then we say:
  - A is the ***domain*** of f
  - B is the ***codomain*** of f
  - b is the ***image*** of a under f
    - a can not have more than 1 image
  - a is a ***pre-image*** of b under f
    - b may have more than 1 pre-image
  - The ***range*** $R \subseteq B$ of f is $R = \{b \mid \exists a\ f(a) = b\}$



Range versus Codomain

- The range of a function might *not* be its whole codomain.
- The codomain is the set that the function is *declared* to map all domain values into.
- The range is the *particular* set of values in the codomain that the function *actually* maps elements of the domain to.

Range vs. Codomain: Example

- Suppose I declare that: "*f* is a function mapping students in this class to the set of grades {A, B, C, D, F}."
- At this point, you know *f* 's codomain is: {A, B, C, D, F}, and its range is unknown!
- Suppose the grades turn out all As and Bs.
- Then the range of *f* is {A, B}, but its codomain is still {A, B, C, D, F}!

Function Operators

- $+$, $\times$ (“plus”,“times”) are binary operators over **R**. (Normal addition & multiplication.)
- Therefore, we can also add and multiply two *real-valued functions* f,g: $\mathbf{R} \to \mathbf{R}$:
  - $(f+g)$: $\mathbf{R} \to \mathbf{R}$, where $(f+g)(x) = f(x) + g(x)$
  - (fg): $\mathbf{R} \to \mathbf{R}$, where $(fg)(x) = f(x)g(x)$
- Example 6:
  Let f and g be functions from **R** to **R** such that $f(x) = x^2$ and $g(x) = x - x^2$.
  What are the functions $f + g$ and fg?

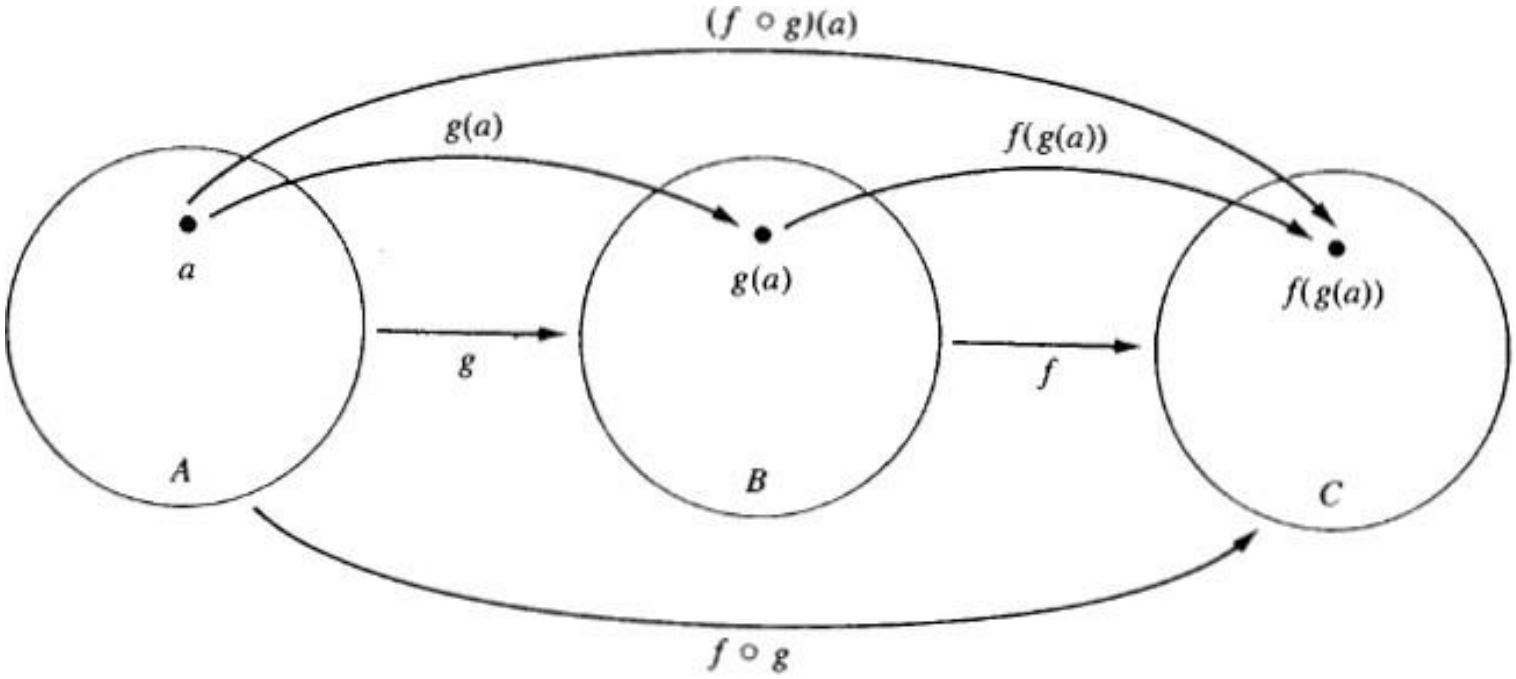
Function Composition Operator

Note the match here. It's necessary!

- For functions g: $A \to B$ and f : $B \to C$, there is a special operator called ***compose*** ("$\circ$").
  - It composes (creates) a new function from f and g by applying f to the result of applying g.
  - We say $(f \circ g)$: $A \to C$, where $(f \circ g)(a) = f(g(a))$.
  - Note: $f \circ g$ cannot be defined unless range of g is a subset of the domain of f.
  - Note $g(a) \in B$, so $f(g(a))$ is defined and $\in C$.
  - Note that $\circ$ is non-commuting. (Like Cartesian $\times$, but unlike +, $\wedge$, $\cup$) (Generally, $f \circ g \neq g \circ f$.)

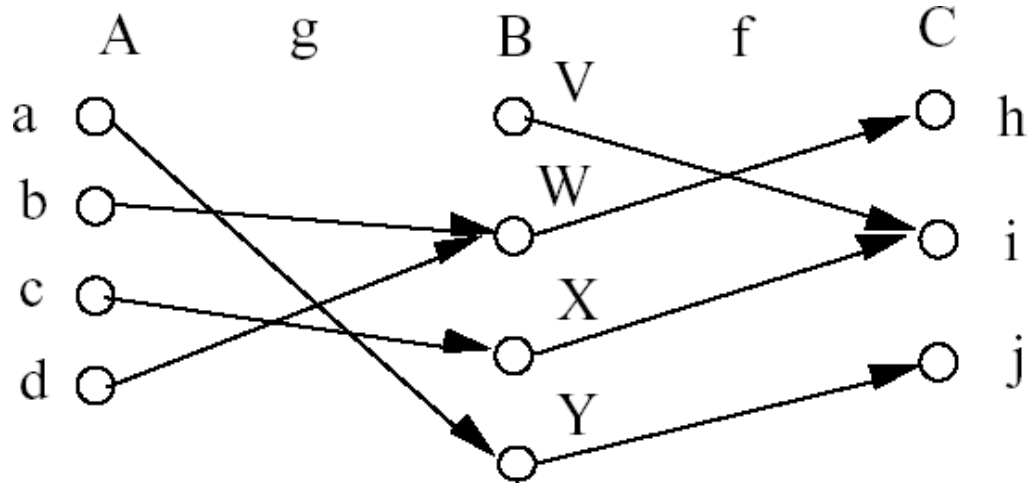
Function Composition Illustration

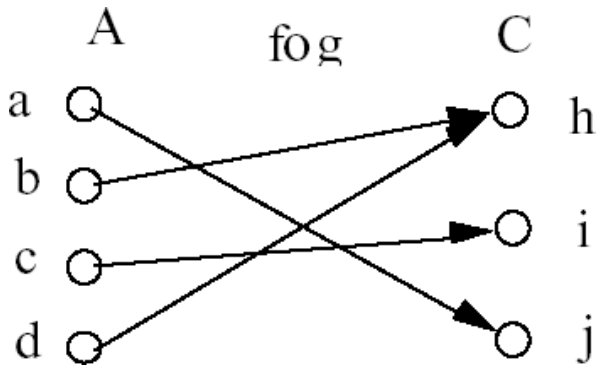
- $g: A \to B, \quad f : B \to C$



Function Composition: Example

- $g: A \rightarrow B, \quad f: B \rightarrow C$





Function Composition: Example

- Example 20: Let g: $\{a, b, c\} \rightarrow \{a, b, c\}$ such that
  $g(a) = b$, $g(b) = c$, $g(c) = a$.

  Let f : $\{a, b, c\} \rightarrow \{1, 2, 3\}$ such that
  $f(a) = 3$, $f(b) = 2$, $f(c) = 1$.

  What is the composition of f and g, and what is the composition of g and f ?

  - $f \circ g$: $\{a, b, c\} \rightarrow \{1, 2, 3\}$ such that
    $(f \circ g)(a) = 2$, $(f \circ g)(b) = 1$, $(f \circ g)(c) = 3$.

    $(f \circ g)(a) = f(g(a)) = f(b) = 2$
    $(f \circ g)(b) = f(g(b)) = f(c) = 1$
    $(f \circ g)(c) = f(g(c)) = f(a) = 3$

  - $g \circ f$ is not defined (why?)

Function Composition: Example

- If $f(x) = x^2$ and $g(x) = 2x + 1$, then what is the composition of f and g, and what is the composition of g and f ?
  - $(f \circ g)(x) = f(g(x))$
    $= f(2x+1)$
    $= (2x+1)^2$
  - $(g \circ f)(x) = g(f(x))$
    $= g(x^2)$
    $= 2x^2 + 1$

  Note that $f \circ g \neq g \circ f$. $(4x^2+4x+1 \neq 2x^2+1)$

Images of Sets under Functions

- Given $f : A \to B$, and $S \subseteq A$,
- The ***image*** of S under f is simply the set of all images (under f) of the elements of S.

$$f(S) = \{f(t) \mid t \in S\}$$
$$= \{b \mid \exists t \in S: f(t) = b\}.$$

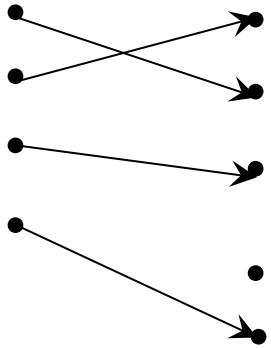
- Note the range of f can be defined as simply the image (under f) of f 's domain.

One-to-One Functions

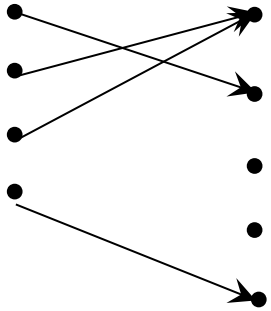
- A function *f* is ***one-to-one*** (*1–1*), or ***injective***, or an ***injection***, iff $f(a) = f(b)$ implies that $a = b$ for all *a* and *b* in the domain of *f* (i.e. every element of its range has *only* 1 pre-image).
  - Formally, given $f : A \rightarrow B$,
    "*f* is injective": $\forall a,b\ (f(a) = f(b) \rightarrow a = b)$ or equivalently $\forall a,b\ (a \neq b \rightarrow f(a) \neq f(b))$
- Only <u>one</u> element of the domain is mapped <u>to</u> any given <u>one</u> element of the range.
  - Domain & range have the same cardinality. What about codomain?

One-to-One Illustration

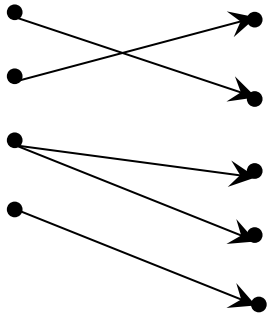
- Bipartite (2-part) graph representations of functions that are (or not) one-to-one:



One-to-one



Not one-to-one



Not even a function!

Example 8:

Is the function $f : \{a, b, c, d\} \rightarrow \{1, 2, 3, 4, 5\}$ with
$f(a) = 4$, $f(b) = 5$, $f(c) = 1$, and $f(d) = 3$ one-to-one?

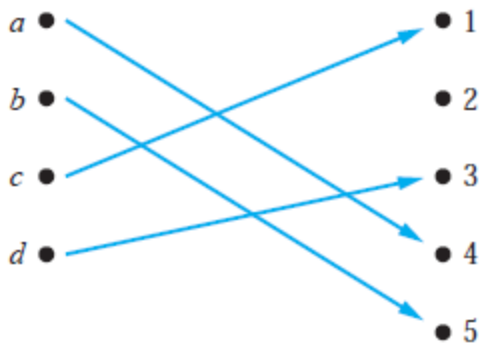


FIGURE 3 A One-to-One Function.

Example 9:

Let $f : \mathbf{Z} \rightarrow \mathbf{Z}$ such that $f(x) = x^2$. Is f one-to-one?

*Solution: The function f (x) = x2 is not one-to-one because, for instance, f (1) = f (−1) = 1,*but 1 = −1.

Note that the function *f (x) = x2 with its domain restricted to* ***Z+ is one-to-one. (Technically,*** when we restrict the domain of a function, we obtain a new function whose values agree with those of the original function for the elements of the restricted domain. The restricted function is not defined for elements of the original domain outside of the restricted domain.)

Sufficient Conditions for 1–1ness

- For functions *f* over numbers, we say:
  - *f* is ***strictly*** (or ***monotonically***) ***increasing*** iff $x > y \rightarrow f(x) > f(y)$ for all *x, y* in domain;
  - *f* is ***strictly*** (or ***monotonically***) ***decreasing*** iff $x > y \rightarrow f(x) < f(y)$ for all *x, y* in domain;

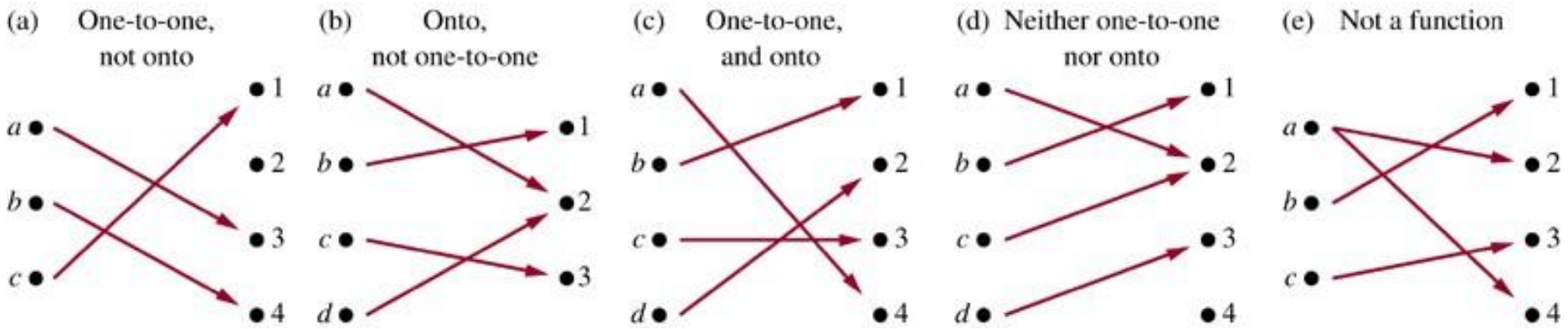
- If *f* is either strictly increasing or strictly decreasing, then *f* is one-to-one.
  - *E.g.* x^3

Onto (Surjective) Functions

- A function $f : A \to B$ is ***onto*** or ***surjective*** or a ***surjection*** iff for every element $b \in B$ there is an element $a \in A$ with $f(a) = b$ ($\forall b \in B, \exists a \in A: f(a) = b$) (i.e. its range is equal to its codomain).
- Think: An *onto* function maps the set A onto (over, covering) the *entirety* of the set B, not just over a piece of it.
- *E.g.*, for domain & codomain **R**, x^3 is onto, whereas x^2 isn't. (Why not?)

Illustration of Onto

- Some functions that are, or are not, *onto* their codomains:



- Example13: Is the function $f(x) = x + 1$ from the set of integers to the set of integers onto?

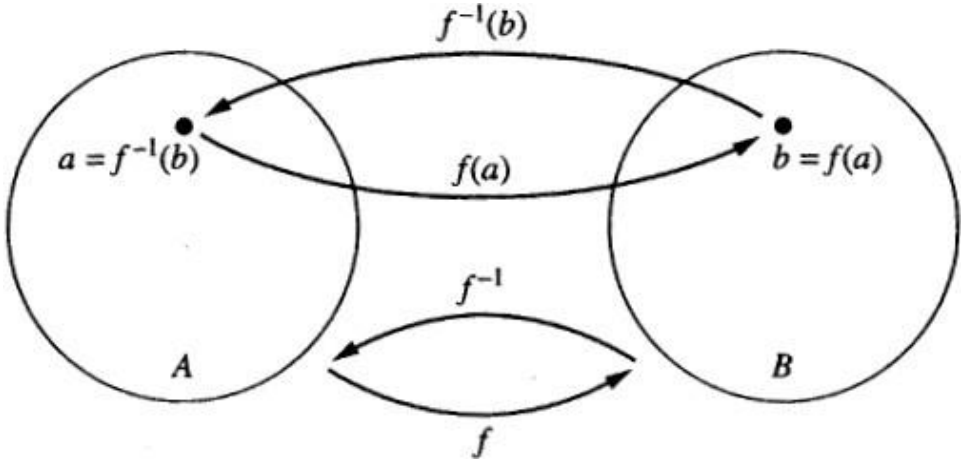
Bijections and Inverse Function

- A function f is said to be *a* ***one-to-one correspondence***, or *a* ***bijection***, or *reversible*, or *invertible*, iff it is both one-to-one and onto.

- Let $f : A \rightarrow B$ be a bijection.
  The ***inverse function*** of f is the function that assigns to an element $b \in B$ the unique element $a \in A$ such that $f(a) = b$.
  The inverse function of f is denoted by $f^{-1}: B \rightarrow A$.
  Hence, $f^{-1}(b) = a$ when $f(a) = b$.

Inverse Function Illustration

- Let $f: A \to B$ be a bijection



- Example 16: Let $f : \{a, b, c\} \to \{1, 2, 3\}$ such that $f(a) = 2$, $f(b) = 3$, $f(c) = 1$. Is f invertible, and if it is, what is its inverse?

  Yes. $f^{-1}(1) = c$, $f^{-1}(2) = a$, $f^{-1}(3) = b$

- Example 18: Let f be the function from **R** to **R** with $f(x) = x^2$. Is f invertible?

  No. f is not a one-to-one function. So it's not invertible.

Mappings in Java

- A discrete function can be represented by a `Map` interface or `HashMap` class in Java programming language
  - `Map map<Integer,String>`
    `= new HashMap<Integer,String>();`
  - Here, the domain is `Integer`, the codomain is `String`
- We can construct such a mapping by putting all pairs {a, f(a)} into our `map`. (a is the *key*, f(a) is the *value*.)
  - `map.put(2,"Jan");`
  - `for (Kid kid:kids) {map.put(kid.id,kid.name);}`
- If we put another pair with the same key, it will overwrite the previous pair – it's not a function! (May be a bug…)

Image, Range, Bijection in Java

- `Map.keys()` returns the **image**
  - it's a Java `Set`!
- `map.values()` returns the **range**
  - it's a Java `Set`!
- Is a `map` a bijection?
  Iff the cardinalities of the **image** and **range** are the same:
  - ```
    if (map.keys().size()==map.values().size()) {
      System.out.println("map is a bijection");
    }
    ```
    ```

Inverse Function in Java

- Let's construct an inverse!
- Prepare the inverse function:
  - `Map inverse<String,Integer>`
    `= new HashMap<String,Integer>();`
  - Here, the domain is `String`, the codomain is `Integer`
- Go through all keys in `map` (all elements of the **image**) and put each pair {value,key} into `inverse`:
  - ```
    for (Integer id:map.keys()) {
      String name = map.get(id);
      inverse.put(id:name,id);
    }
    ```
    ```

Summation Notation

- Given a sequence $\{a_n\}$, an integer *lower bound* (or *limit*) $j \geq 0$, and an integer *upper bound* $k \geq j$, then the *summation of* $\{a_n\}$ *from* a_j *to* a_k is written and defined as follows:

$$\sum_{i=j}^{k} a_i = a_j + a_{j+1} + \ldots + a_k$$

- Here, *i* is called the *index of summation*.

$$\sum_{i=j}^{k} a_i = \sum_{m=j}^{k} a_m = \sum_{l=j}^{k} a_l$$

Generalized Summations

- For an infinite sequence, we write:

$$\sum_{i=j}^{\infty} a_i = a_j + a_{j+1} + \cdots$$

- To sum a function over all members of a set $X = \{x_1, x_2, \ldots\}$:

$$\sum_{x \in X} f(x) = f(x_1) + f(x_2) + \cdots$$

- Or, if $X = \{x \mid P(x)\}$, we may just write:

$$\sum_{P(x)} f(x) = f(x_1) + f(x_2) + \cdots$$

Simple Summation Example

- $\sum_{i=2}^{4}\left(i^2+1\right)=$

- $1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}\cdots+\frac{1}{100}=\sum_{i=1}^{100}\frac{1}{i}$

More Summation Examples

- An infinite sequence with a finite sum:

$$\sum_{i=0}^{\infty} 2^{-i} = 2^0 + 2^{-1} + \cdots = 1 + \frac{1}{2} + \frac{1}{4} + \cdots = 2$$

- Using a predicate to define a set of elements to sum over:

$$\sum_{\substack{(x \text{ is prime}) \wedge \\ x<10}} x^2 = 2^2 + 3^2 + 5^2 + 7^2$$

$$= 4 + 9 + 25 + 49 = 87$$

Summation Manipulations

- Some handy identities for summations:
  - Summing constant value

$$\sum_{n=i}^{j} c = (j - i + 1) \cdot c$$

Number of terms in the summation

$$\sum_{n=1}^{3} 2 =$$

$$= \text{ʊ}$$

$$\sum_{n=-1}^{2} 2i$$

$$= 4 \oplus (2i) = 8i$$

Summation Manipulations

- Distributive law

$$\sum_{n=i}^{j} cf(n) = c\sum_{n=i}^{j} f(n)$$

$$\sum_{n=1}^{3}\left(4\cdot n^2\right) = 4\cdot 1^2 + 4\cdot 2^2 + 4\cdot 3^2$$

$$= 4\cdot\left(1^2 + 2^2 + 3^2\right)$$

$$= 4\sum_{n=1}^{3} n^2$$

Summation Manipulations

- An application of commutativity

$$\sum_{n=i}^{j}\left(f(n)+g(n)\right)=\sum_{n=i}^{j}f(n)+\sum_{n=i}^{j}g(n)$$

$$\sum_{n=2}^{4}(n+2n)=(2+2\cdot 2)+(3+2\cdot 3)+(4+2\cdot 4)$$

$$=(2+3+4)+(2\cdot 2+2\cdot 3+2\cdot 4)$$

$$=\sum_{n=2}^{4}n+\sum_{n=2}^{4}2n$$

Index Shifting

$$\sum_{i=j}^{m} f(i) = \sum_{k=j+n}^{m+n} f(k-n)$$

$$\sum_{i=1}^{4} i^2 = 1^2 + 2^2 + 3^2 + 4^2$$

- Let $k = i + 2$, then $i = k - 2$

$$\sum_{k=1+2}^{4+2} (k-2)^2 = \sum_{k=3}^{6} (k-2)^2$$

$$= (3-2)^2 + (4-2)^2 + (5-2)^2 + (6-2)^2$$

More Summation Manipulations

- Sequence splitting

$$\sum_{i=j}^{k} f(i) = \sum_{i=j}^{m} f(i) + \sum_{i=m+1}^{k} f(i) \quad \text{if } j \le m < k$$

$$\sum_{i=0}^{4} i^3 = 0^3 + 1^3 + 2^3 + 3^3 + 4^3$$

$$= (0^3 + 1^3 + 2^3) + (3^3 + 4^3)$$

$$= \sum_{i=0}^{2} i^3 + \sum_{i=3}^{4} i^3$$

More Summation Manipulations

- Order reversal

$$\sum_{i=0}^{k} f(i) = \sum_{i=0}^{k} f(k-i)$$

$$\sum_{i=0}^{3} i^3 = 0^3 + 1^3 + 2^3 + 3^3$$

$$= (3-0)^3 + (3-1)^3 + (3-2)^3 + (3-3)^3$$

$$= \sum_{i=0}^{3} (3-i)^3$$

Example: Geometric Progression

- A *geometric progression* is a sequence of the form a, ar, ar^2, ar^3, …, ar^n ,… where $a,r \in \mathbf{R}$.
- The sum of such a sequence is given by:

$$S = \sum_{i=0}^{n} ar^i$$

- We can reduce this to *closed form* via clever manipulation of summations...

THEOREM 1 If a and r are real numbers and $r \neq 0$, then

$$\sum_{j=0}^{n} ar^j = \begin{cases} \dfrac{ar^{n+1} - a}{r - 1} & \text{if } r \neq 1 \\ (n+1)a & \text{if } r = 1. \end{cases}$$

Proof: Let

$$S_n = \sum_{}^{n} ar^j.$$

To compute S, first multiply both sides of the equality by r and then manipulate the resulti sum as follows:

$$
\begin{aligned}
r S_n &= r \sum_{j=0}^{n} ar^j && \text{substituting summation formula for } S \\
&= \sum_{j=0}^{n} ar^{j+1} && \text{by the distributive property} \\
&= \sum_{k=1}^{n+1} ar^k && \text{shifting the index of summation, with } k = j + 1 \\
&= \left(\sum_{k=0}^{n} ar^k \right) + (ar^{n+1} - a) && \text{removing } k = n + 1 \text{ term and adding } k = 0 \text{ term} \\
&= S_n + (ar^{n+1} - a) && \text{substituting } S \text{ for summation formula}
\end{aligned}
$$

From these equalities, we see that

$$rS_n = S_n + (ar^{n+1} - a).$$

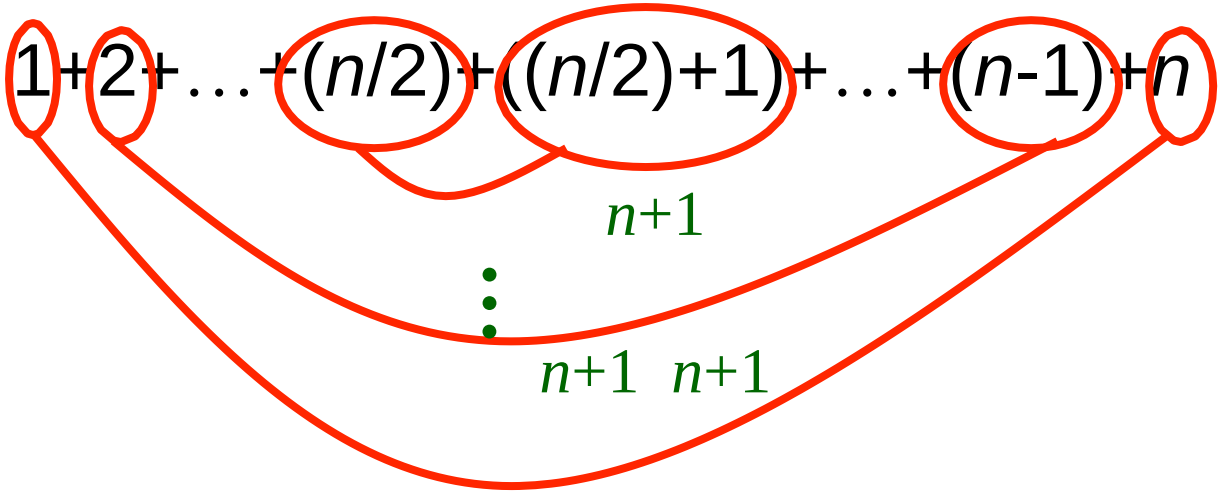
Solving for S_n shows that if $r \neq 1$, then

$$S_n = \frac{ar^{n+1} - a}{r - 1}.$$

If $r = 1$, then the $S_n = \sum_{j=0}^{n} ar^j = \sum_{j=0}^{n} a = (n + 1)a$.

Gauss' Trick, Illustrated

- Consider the sum:



- We have $n/2$ pairs of elements, each pair summing to $n+1$, for a total of $(n/2)(n+1)$.

Some Shortcut Expressions

TABLE 2 Some Useful Summation Formulae.

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

Using the Shortcuts

- Example: Evaluate $\sum_{k=50}^{100} k^2$

- Use series splitting.

  - Solve for desired summation.

  - Apply quadratic series rule.

  - Evaluate.

$$\sum_{k=1}^{100} k^2 = \left(\sum_{k=1}^{100} k^2\right) - \left(\sum_{k=1}^{49} k^2\right)$$

$$\sum_{k=50}^{100} k^2 = \left(\sum_{k=1}^{100} k^2\right) - \left(\sum_{k=1}^{49} k^2\right)$$

$$= \frac{100 \cdot 101 \cdot 201}{6} - \frac{49 \cdot 50 \cdot 99}{6}$$

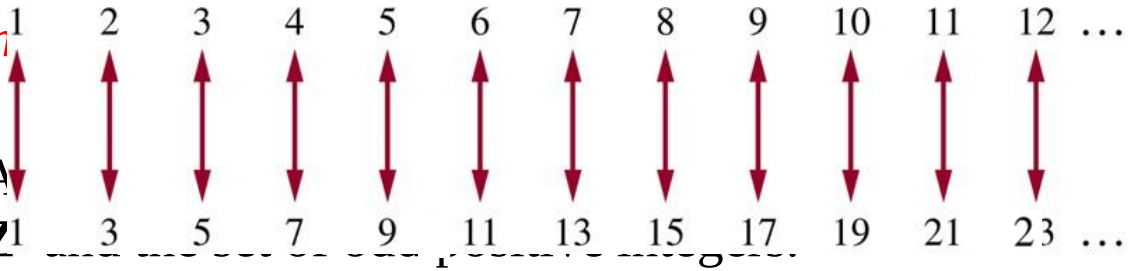
$$= 338{,}350 - 40{,}425$$

$$= 297{,}925.$$

Cardinality

- The sets *A* and *B* have the same ***cardinality*** if and only if there is a one-to-one correspondence from *A* to *B*.
- A set that is either finite or has the same cardinality as the set of positive integers is called **countable**.
- A set that is not countable is called **uncountable**.
- Example: Show that the set of odd positive integers is a countable set.

Consider the function $f(n)$ = $2n - 1$ from the set of positive integers



between **Z**

Summation Manipulations

- Useful identities:

$$\sum_{i=j}^{k} f(i) = \sum_{i=j}^{m} f(i) + \sum_{i=m+1}^{k} f(i) \quad \text{if } j \le m < k$$

(Sequence splitting.)

$$\sum_{i=0}^{k} f(i) = \sum_{i=0}^{k} f(k-i)$$

(Order reversal.)

$$\sum_{i=1}^{2k} f(i) = \sum_{i=1}^{k} \left(f(2i-1) + f(2i) \right)$$

(Grouping.)

Chapter 3. The Fundamentals

4. The Integers and Division
5. Primes and Greatest Common Divisors

The Division "Algorithm"

- It's really just a *theorem*, not an algorithm…
- Only called an "algorithm" for historical reasons.

- **Theorem:** For any integer ***dividend*** a and ***divisor*** $d \in \mathbf{Z}^+$, there are unique integers ***quotient*** q and ***remainder*** $r \in \mathbf{N}$ such that $a = dq + r$ and $0 \leq r < d$.

$q = a$ ***div d, r = a mod d.***

The mod Operator

- An integer "division remainder" operator.
- Let $a, d \in \mathbf{Z}$ with $d > 1$. Then a **mod** d denotes the remainder r from the division "algorithm" with dividend a and divisor d; i.e. the remainder when a is divided by d.
  Also, a **div** d denotes the quotient q.
- We can compute (a **mod** d) by:

$$a - d \cdot$$

- In C/C++/Java languages, "%" = mod.

The mod Operator: Examples

- 101 = 11·9 + 2 (dividend: 101, divisor: 11)
  - 101 **div** 11 = 9 101 **mod** 11 = 2

- –11 = 3·(–4) + 1 or ~~–11 = 3·(–3) – 2 ?~~
  (dividend: –11, divisor: 3)
  - –11 **div** 3 = –4 –11 **mod** 3 = 1
    (quotient: –4, remainder: 1)

- Note that the remainder must not be negative.

Modular Congruence

- Let $a,b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$, where $\mathbf{Z}^+ = \{n \in \mathbf{Z} \mid n > 0\} = \mathbf{N} - \{0\}$ (the positive integers).
- Then ***a is congruent to b modulo m***, written "$a \equiv b$ (**mod** m)", iff $m|(a - b)$.
- Note: this is a different use of "≡" than the meaning "equivalent" or "is defined as" used before.
- It's also equivalent to: $(a - b)$ **mod** $m = 0$.
- E.g. $17 \equiv 5$ (**mod** 6), $24 \not\equiv 14$ (**mod** 6)

Useful Congruence Theorems

- **Theorem:** Let $a,b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then:

  $a \equiv b \pmod{m} \Leftrightarrow a \bmod m = b \bmod m$.

- **Theorem:** Let $a,b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then:

  $a \equiv b \pmod{m} \Leftrightarrow \exists k \in \mathbf{Z}: a = b + km$.

Proof: If a ≡ b (mod m), by the definition of congruence we know that *m | (a − b). This means that there is an integer k such that a − b = km, so that a = b + km.*

Conversely, if there is an integer *k such that a = b + km, then km = a − b. Hence, m divides a − b, so that a ≡ b (mod m).*

- **Theorem:** Let $a,b,c,d \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:

Theorem: Let $a,b,c,d \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:

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

Proof:We use a direct proof. Because a ≡ b (mod m) and c ≡ d (mod m), by Theorem 4 there are integers *s and t with b = a + sm and d = c + tm. Hence,*

$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$

and

$bd = (a + sm)(c + tm) = ac + m(at + cs + stm).$

Hence,

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

Congruence Theorem Example

- $7 \equiv 2$ (**mod** 5) and $11 \equiv 1$ (**mod** 5).
  - $7 + 11 = 18$ and $2 + 1 = 3$

    Therefore, $7 + 11 \equiv 2 + 1$ (**mod** 5)
  - $7 \times 11 = 77$ and $2 \times 1 = 2$

    Therefore, $7 \times 11 \equiv 2 \times 1$ (**mod** 5)

Applications of Congruence

- Hashing Functions (hashes)
- Pseudorandom Numbers
- Cryptology
- Universal Product Codes
- International Standard Book Numbers

Hashing Functions

- We want to quickly store and retrieve records in memory locations.
- A hashing function takes a data item to be stored or retrieved and computes the first choice for a location for the item.
- $h(k) = k \bmod m$
- A hashing function h assigns memory location $h(k)$ to the record that has k as its key.
- $h(064212848) = 064212848 \bmod 111 = 14$
- $h(037149212) = 037149212 \bmod 111 = 65$
- $h(107405723) = 107405723 \bmod 111 = 14 \quad \Rightarrow$ collision!
- Find the first unoccupied memory location after the occupied memory.
- In this case, assign memory location 15.
- If collision occurs infrequently, and if when one does occur it is resolved quickly, then hashing provides a very fast method of storing and retrieving data.

Cryptology (I)

- The study of secret messages

- **Encryption** is the process of making a message secret. **Decryption** is the process of determining the original message from the encrypted message.

- Some simple early codes include *Caesar's cipher*:
  - Assign an integer from 0 to 25 to each letter based on its position in the alphabet.
  - Caesar's encryption method: $f(p) = (p + 3)$ **mod** 26
  - Caesar's decryption method: $f^{-1}(p) = (p - 3)$ **mod** 26
  - MEET YOU IN THE PARK $\Rightarrow$
PHHW BRX LQ WKH SDUN

EXAMPLE

What is the secret message produced from the message “MEET YOU IN THE PARK” using
the Caesar cipher?

Solution: First replace the letters in the message with numbers. This produces

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.***

This gives

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

Translating this back to letters produces the encrypted message “PHHW BRX LQ WKH SDUN.”

Cryptology (II)

- Caesar's encryption method does not provide a high level of security
- A slightly better approach: $f(p) = (ap + b) \bmod 26$

- **Example 10:**

What letter replaces the letter *K* when the function $f(p) = (7p + 3) \bmod 26$ is used for encryption?

- 10 represents *K*
- $f(10) = (7 \times 10 + 3) \bmod 26 = 73 \bmod 26 = 21$
- 21 represents *V*
- Therefore, *K* is replaced by *V* in the encrypted message

Prime Numbers

- An integer $p > 1$ is ***prime*** iff the only positive factors of *p* are 1 and *p* itself.
- Some primes: 2, 3, 5, 7, 11, 13,...
- Non-prime integers greater than 1 are called ***composite***, because they can be *composed* by multiplying two integers greater than 1.

The Fundamental Theorem of Arithmetic

Its "Prime Factorization"

- Every positive integer greater than 1 has a *unique* representation as a prime or as the product of a non-decreasing series of two or more primes.
- Some examples:
  - 2 = 2 (a prime 2)
  - $4 = 2 \cdot 2 = 2^2$ (product of series 2, 2)
  - $2000 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 5 = 2^4 \cdot 5^3$ $2001 = 3 \cdot 23 \cdot 29$

$2002 = 2 \cdot 7 \cdot 11 \cdot 13$

2003 = 2003 (no clear pattern!)

Prime Numbers: Theorems

- Contrapositive of Theorem 2:

  An integer is prime if it is not divisible by any prime less than or equal to its square root $\sqrt{n}$

- Example: Show that 101 is prime
  - Primes not exceeding $\sqrt{101}$: 2, 3, 5, 7
  - 101 is not divisible by any of 2, 3, 5, or 7
  - Therefore, 101 is a prime

Prime Factorization

- **Example 4**: Find the prime factorization of 7007 ($\sqrt{7007} \approx 83.7$)
  - Perform division of 7007 by successive primes

    7007 / 7 = 1001 (7007 = 7·1001)
  - Perform division of 1001 by successive primes beginning with 7

    1001 / 7 = 143 (7007 = 7·7·143)
  - Perform division of 143 by successive primes beginning with 7

    143 / 11 = 13 (7007 = 7·7·11·13

    = 7^2·11·13)

Greatest Common Divisor

- The ***greatest common divisor*** gcd(a,b) of integers a, b is the largest integer d that is a divisor both of a and of b.

$d = \gcd(a,b) = \max(d: d|a \wedge d|b)$

$\Leftrightarrow d|a \wedge d|b \wedge \forall e \in \mathbf{Z}, (e|a \wedge e|b) \rightarrow (d \geq e)$

- **Example:** gcd(24,36) = ?
- Positive divisors of 24: 1, 2, 3, 4, 6, 8, 12, 24
- Positive divisors of 36: 1, 2, 3, 4, 6, 9, 12, 18, 36
- Positive common divisors: 1, 2, 3, 4, 6, 12.

The largest one of these is 12.

Relative Primality

- Integers *a* and *b* are called ***relatively prime*** or ***coprime*** iff their gcd = 1.

- **Example:** Neither 21 nor 10 is prime, but they are *relatively prime*. (divisors of 21: 1, 3, 7, 21; divisors of 10: 1, 2, 5, 10; so they have no common factors $>$ 1, so their gcd = 1.

- A *set* of integers $\{a_1, a_2, a_3, \ldots\}$ is ***pairwise relatively prime*** if all pairs (a_i, a_j), for $i \neq j$, are relatively prime.

GCD Shortcut

- If the prime factorizations are written as

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

  then the GCD is given by:

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

- Example of using the shortcut:
  - a = 84 = 2·2·3·7 = $2^2 \cdot 3^1 \cdot 7^1$
  - b = 96 = 2·2·2·2·2·3 = $2^5 \cdot 3^1 \cdot 7^0$
  - gcd(84,96) = $2^2 \cdot 3^1 \cdot 7^0$ = 2·2·3 = 12.

Least Common Multiple

- lcm(a,b) of positive integers a, b, is the smallest positive integer that is a multiple both of a and of b. *E.g.* lcm(6,10) = 30

$m = \text{lcm}(a,b) = \min(m: a|m \wedge b|m)$

$\Leftrightarrow a|m \wedge b|m \wedge \forall n \in \mathbf{Z}: (a|n \wedge b|n) \rightarrow (m \leq n)$

- **Example:** lcm(24,36) = ?
- Positive multiples of 24: 24, 48, 72, 96, 120, 144,…
- Positive multiples of 36: 36, 72, 108, 144,…
- Positive common multiples: 72, 144,… The smallest one of these is 72.

LCM Shortcut

- If the prime factorizations are written as $a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$, then the LCM is given by

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

- Example of using the shortcut:
  - $a = 84 = 2 \cdot 2 \cdot 3 \cdot 7 = 2^2 \cdot 3^1 \cdot 7^1$
  - $b = 96 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^5 \cdot 3^1 \cdot 7^0$
  - $\text{lcm}(84,96) = 2^5 \cdot 3^1 \cdot 7^1 = 32 \cdot 3 \cdot 7 = 672$

LCM: Another Example

- Example 15:

What is the least common multiple of $2^3 \cdot 3^5 \cdot 7^2$ and $2^4 \cdot 3^3$?

- Solution: lcm($2^3 \cdot 3^5 \cdot 7^2$, $2^4 \cdot 3^3$)

$= 2^{\max(3,4)} \cdot 3^{\max(5,3)} \cdot 7^{\max(2,0)}$

$= 2^4 \cdot 3^5 \cdot 7^2$

GCD and LCM

- **Theorem**: Let a and b be positive integers. Then

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

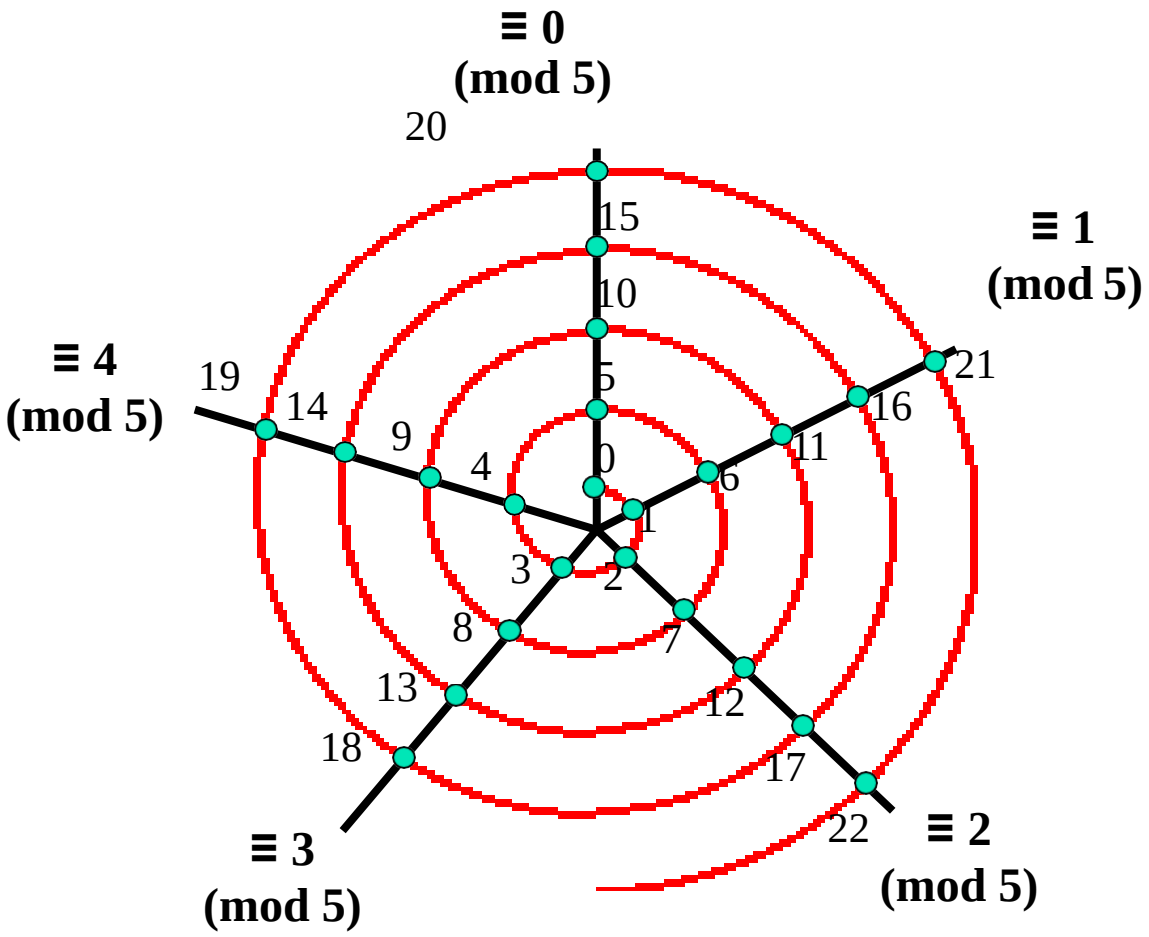
- Example
  - $a = 84 = 2 \cdot 2 \cdot 3 \cdot 7 = 2^2 \cdot 3^1 \cdot 7^1$
  - $b = 96 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^5 \cdot 3^1 \cdot 7^0$
  - $ab = (2^2 \cdot 3^1 \cdot 7^1) \cdot (2^5 \cdot 3^1 \cdot 7^0) = 2^2 \cdot 3^1 \cdot 7^0 \cdot 2^5 \cdot 3^1 \cdot 7^1$

$= 2^{\min(2,5)} \cdot 3^{\min(1,1)} \cdot 7^{\min(1,0)} \cdot 2^{\max(2,5)} \cdot 3^{\max(1,1)} \cdot 7^{\max(1,0)}$

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

Spiral Visualization of mod

- Example shown: modulo-5 arithmetic



Pseudorandom Numbers

- Randomly chosen numbers are often needed for computer simulations.
- Different methods have been devised for generating numbers that have properties of randomly chosen numbers.
- Because numbers generated by systematic methods are not truly random, they are called **pseudorandom numbers.**
- The most commonly used procedure for generating pseudorandom numbers is the **linear congruential method.**

Linear Congruential Method

- Requires four natural numbers:
  - The *modulus m,* the *multiplier a*, the *increment c*, and the *seed* x_0.
- where $2 \le a < m$, $0 \le c < m$, $0 \le x_0 < m$.
- Generates the pseudo-random sequence $\{x_n\}$ with $0 \le x_n < m$, via the following:

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

- Tends to work best when *a*, *c*, *m* are prime, or at least relatively prime.
- If $c = 0$, the method is called a *pure multiplicative generator*.

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 x0 = 3.*

Solution:We compute the terms of this sequence by successively using the recursively defined

function *xn+1 = (7xn + 4)* ***mod 9, beginning by inserting the seed x0 = 3 to find x1. We find***

that

x1 = 7x0 + 4 ***mod 9 = 7 · 3 + 4 mod 9 = 25 mod 9 = 7,***

x2 = 7x1 + 4 ***mod 9 = 7 · 7 + 4 mod 9 = 53 mod 9 = 8,***

x3 = 7x2 + 4 ***mod 9 = 7 · 8 + 4 mod 9 = 60 mod 9 = 6,***

$x4 = 7x3 + 4 \bmod 9 = 7 \cdot 6 + 4 \bmod 9 = 46 \bmod 9 = 1,$

$x5 = 7x4 + 4 \bmod 9 = 7 \cdot 1 + 4 \bmod 9 = 11 \bmod 9 = 2,$

$x6 = 7x5 + 4 \bmod 9 = 7 \cdot 2 + 4 \bmod 9 = 18 \bmod 9 = 0,$

$x7 = 7x6 + 4 \bmod 9 = 7 \cdot 0 + 4 \bmod 9 = 4 \bmod 9 = 4,$

$x8 = 7x7 + 4 \bmod 9 = 7 \cdot 4 + 4 \bmod 9 = 32 \bmod 9 = 5,$

$x9 = 7x8 + 4 \bmod 9 = 7 \cdot 5 + 4 \bmod 9 = 39 \bmod 9 = 3.$

Because *x9 = x0 and because each term depends only on the previous term, we see that the* sequence

3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, . . .

is generated. This sequence contains nine different numbers before repeating.

Mersenne Primes

- **Definition**: A ***Mersenne prime*** is a prime number of the form $2^p - 1$, where p is prime.

prime p	$2^p - 1$	Mersenne?
2	$2^2 - 1 = 3$	yes
3	$2^3 - 1 = 7$	yes
5	$2^5 - 1 = 31$	yes
7	$2^7 - 1 = 127$	yes
11,213	$2^{11,213} - 1$	yes
19,937	$2^{19,937} - 1$	yes
3,021,377	$2^{3,021,377} - 1$	Yes (late 1998)
43,112,609	$2^{43,112,609} - 1$	Yes (MID 2008)

largest Mersenne prime known (with almost 13 million digits)

Chapter 3. The Fundamentals

3.6 Applications of Integers Algorithms

Euclid's Algorithm for GCD

- Finding GCDs by comparing prime factorizations can be difficult when the prime factors are not known!

•More efficient method of finding gcd is the called the **Euclidean algorithm**

- **Euclid discovered:** Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a,b) = \gcd(b,r)$ (i.e. $\gcd(a,b) = \gcd(b, (a \bmod b))$)
  - Example: gcd(36, 24) = gcd(24, 12)
- Sort a, b so that $a > b$, and then (given $b > 1$) $(a \bmod b) < b$, so problem is simplified.

The Euclidean Algorithm

•**Example:**

gcd*(91, 287).*

First, divide 287, the larger of the two integers, by 91, the smaller, to obtain $287 = 91 \cdot 3 + 14$.

Any divisor of 91 and 287 must also be a divisor of $287 - 91 \cdot 3 = 14$.

any divisor of 91 and 14 must also be a divisor of $287 = 91 \cdot 3 + 14$.

Hence, the gcd(91,287) is the same as the gcd(91,14)

i.e. finding gcd*(91, 287) reduced to find gcd(91, 14).*

Next, divide 91 by 14 to obtain $91 = 14 \cdot 6 + 7$.

any common divisor of 91 and 14 also divides $91 - 14 \cdot 6 = 7$

and any common divisor of 14 and 7 divides 91,

gcd*(91, 14) = gcd(14, 7).* gcd(14, 7) = 7.

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

Euclid's Algorithm Example

- gcd(372, 164) = gcd(164, 372 mod 164)
  - 372 mod 164 = 372 - 164⌊372/164⌋
    = 372 - 164·2 = 372 - 328 = 44
- gcd(164, 44) = gcd(44, 164 mod 44)
  - 164 mod 44 = 164 - 44⌊164/44⌋
    = 164 - 44·3 = 164 - 132 = 32
- gcd(44, 32) = gcd(32, 44 mod 32) = gcd(32, 12)
  = gcd(12, 32 mod 12) = gcd(12, 8)
  = gcd(8, 12 mod 8) = gcd(8, 4)
  = gcd(4, 8 mod 4) = gcd(4, 0) = 4

Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

Solution: Successive uses of the division algorithm give:

$662 = 414 \cdot 1 + 248$

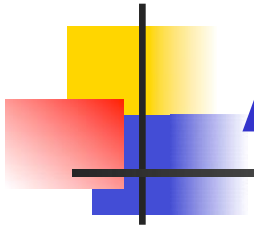
$414 = 248 \cdot 1 + 166$

$248 = 166 \cdot 1 + 82$

$166 = 82 \cdot 2 + 2$

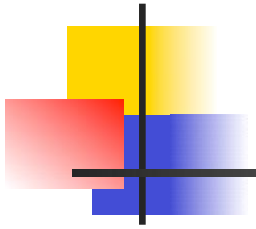
$82 = 2 \cdot 41$.

Hence, gcd(414, 662) = 2, because 2 is the last nonzero remainder.



Applications

- Linear congruences
- Chinese Remainder Theorem
- Public Key Cryptography
  - The Rivest-Shamir-Adleman (RSA) cryptosystem



- **Theorem 1:**
  - $\forall a,b \in \mathbf{Z}^+$: $\exists s,t \in \mathbf{Z}$: $\gcd(a,b) = sa + tb$
- **Lemma 1:**
  - $\forall a,b,c \in \mathbf{Z}^+$: $\gcd(a,b)=1 \wedge a \mid bc \rightarrow a \mid c$
- **Lemma 2:**
  - If p is prime and $p \mid a_1 a_2 \ldots a_n$ (integers a_i) then $\exists i$: $p \mid a_i$.
- **Theorem 2:**
  - If $ac \equiv bc \pmod{m}$ and $\gcd(c,m)=1$, then $a \equiv b \pmod{m}$. ($m \in \mathbf{Z}^+$, $a,b,c \in \mathbf{Z}$)

BÉZOUT'S THEOREM

- $\forall a,b \in \mathbf{Z}^+: \exists s,t \in \mathbf{Z}$ such that $\gcd(a,b) = sa + tb$

  sa + tb, where *s and t are integers.*

  gcd(a, b) can be expressed as a ***linear combination*** with integer coefficients of *a and b.*

  For example, gcd(6, 14) = 2, and 2 = (–2) · 6 + 1 · 14.

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

Theorem 1: Example

- Express gcd(252, 198) = 18 as a linear combination of 252 and 198.
  - $252 = 1 \cdot 198 + 54$
    $198 = 3 \cdot 54 + 36$
    $54 = 1 \cdot 36 + 18$
    $36 = 2 \cdot 18$

    } Euclidean algorithm
  - $18 = 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54)$
    $= 4 \cdot 54 - 1 \cdot 198$
    $= 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198$
    $= 4 \cdot 252 - 5 \cdot 198$
  - Therefore, gcd(252, 198) = $18 = 4 \cdot 252 + (-5) \cdot 198$

Proof of Lemma 1

- **Lemma 1:**

  $\forall a,b,c \in \mathbf{Z}^+: \gcd(a,b)=1 \wedge a|bc \rightarrow a|c$

  Proof:

  - Applying theorem 1, $\exists s, t: sa + tb = 1$.
  - Multiplying through by c, we have that $sac + tbc = c$.
  - Since $a|bc$ is given, we know that $a|tbc$, and obviously $a|sac$.
  - Thus (using the theorem on pp.202), it follows that $a|(sac+tbc)$; in other words, that $a|c$. ■

Proof of Lemma 2

- **Lemma 2:** If p is prime and $p|a_1a_2\ldots a_n$ (integers a_i) then $p|a_i$ for some i.

Proof (by induction):

- If $n=1$, this is immediate since $p|a_0 \rightarrow p|a_0$.
  Suppose the lemma is true for all $n<k$ and $p|a_1\ldots a_k$.
- If $p|m$ where $m=a_1\ldots a_{k-1}$ then we have it inductively.
- Otherwise, we have $p|ma_k$ but $\neg(p|m)$.
  Since m is not a multiple of p, and p has no factors, m has no common factors with p, thus $\gcd(m,p)=1$.
  So by applying Lemma 1, $p|a_k$. ■

Theorem 2

- **Theorem 2:** Let $m \in \mathbf{Z}^+$ and $a,b,c \in \mathbf{Z}$.
  If $ac \equiv bc \pmod{m}$ and $\gcd(c,m)=1$, then $a \equiv b \pmod{m}$.

  Proof:

  - Since $ac \equiv bc \pmod{m}$, this means $m \mid ac-bc$.
  - Factoring the right side, we get $m \mid c(a-b)$.
    Since $\gcd(c,m)=1$, lemma 1 implies that $m \mid a-b$,
    in other words, that $a \equiv b \pmod{m}$. ■

- Examples
  - $20 \equiv 8 \pmod 3$ i.e. $5 \cdot 4 \equiv 2 \cdot 4 \pmod 3$

    Since $\gcd(4, 3) = 1$, $5 \equiv 2 \pmod 3$
  - $14 \equiv 8 \pmod 6$ but $7 \not\equiv 4 \pmod 6$ (as $\gcd(2,6) \neq 1$)

Linear Congruences, Inverses

- A congruence of the form $ax \equiv b \pmod{m}$ is called a ***linear congruence***. ($m \in \mathbf{Z}^+$, $a, b \in \mathbf{Z}$, and x: variable)
  - To *solve* the congruence is to find the x's that satisfy it.
- An ***inverse of a, modulo m*** is any integer a^{-1} such that $a^{-1}a \equiv 1 \pmod{m}$.
  - If we can find such an a^{-1}, notice that we can then solve $ax \equiv b \pmod{m}$ by multiplying through by it, giving $a^{-1}ax \equiv a^{-1}b \pmod{m}$, thus $1 \cdot x \equiv a^{-1}b \pmod{m}$, thus $x \equiv a^{-1}b \pmod{m}$.

Theorem 3

- **Theorem 3:** If $\gcd(a,m)=1$ (i.e. a and m are relatively prime) and $m > 1$,
  then a has a inverse a^{-1} unique modulo m.

  Proof:

  - By theorem 1, $\exists s,t$: $sa + tm = 1$, so $sa + tm \equiv 1 \pmod{m}$.
  - Since $tm \equiv 0 \pmod{m}$, $sa \equiv 1 \pmod{m}$.
    Thus s is an inverse of a (mod m).
  - Theorem 2 guarantees that if $ra \equiv sa \equiv 1$ then $r \equiv s$,
    thus this inverse is unique modulo m.
    (All inverses of a are in the same congruence class as s.)
    ■

Example

- Find an inverse of 3 modulo 7
  - Since gcd(3, 7) = 1, by Theorem 3 there exists an inverse of 3 modulo 7.
  - $7 = 2 \cdot 3 + 1$
  - From the above equation, $-2 \cdot 3 + 1 \cdot 7 = 1$
  - Therefore, –2 is an inverse of 3 modulo 7
  - Note that every integer congruent to –2 modulo 7 is also an inverse of 3, such as 5, –9, 12, and so on.)

Example

- What are the solutions of the linear congruence $3x \equiv 4 \pmod 7$?
  - -2 is an inverse of 3 modulo 7 (previous slide)
  - Multiply both side by -2: $-2 \cdot 3x \equiv -2 \cdot 4 \pmod 7$
  - $-6 \cdot x \equiv x \equiv -8 \equiv 6 \pmod 7$
  - Therefore, the solutions to the congruence are the integers x such that $x \equiv 6 \pmod 7$, i.e. 6, 13, 20, 27,… and –1, –8, –15,…

The Chinese Remainder Theorem

Let *m1,m2, . . . , mn be pairwise relatively*
prime positive integers greater than one and *a1, a2, . . . , an arbitrary integers. Then the system*
$x \equiv a1 \pmod{m1}$,
$x \equiv a2 \pmod{m2}$,
.
.
.
$x \equiv an \pmod{mn}$
has a unique solution modulo $m = m1m2 \cdot \cdot \cdot mn$.
(That is, there is a solution x with
$0 \leq x < m$, *and all other solutions are congruent modulo m to this solution.)*

Proof: To establish this theorem,
we need to show that a solution exists and that it is unique modulo *m. We will show that a solution exists by describing a way to construct this solution;*
showing that the solution is unique modulo *m*
To construct a simultaneous solution,
first let *Mk = m/mk* for *k = 1, 2, . . . , n. i.e., Mk is the product of the moduli except for mk.*
Because mi and mk have no common factors greater than 1 when *i = k, it follows that gcd(mk,Mk) = 1.*
we know that there is an integer *yk, an inverse of Mk modulo mk, such* that *Mkyk ≡ 1 (mod mk).*
To construct a simultaneous solution, form the sum
x = a1M1y1 + a2M2y2 + · · · +anMnyn.

We will now show that *x is a simultaneous solution.*
First, note that because $Mj \equiv 0 \pmod{mk}$
whenever $j = k$, *all terms except the kth term in this sum are congruent to 0 modulomk.*
Because $Mkyk \equiv 1 \pmod{mk}$
$x \equiv akMkyk \equiv ak \pmod{mk}$, for $k = 1, 2, \ldots, n$.
So x is a simultaneous solution to the n congruences.
What are the solutions of the systems of congruences
$x \equiv 2 \pmod{3}$,
$x \equiv 3 \pmod{5}$,
$x \equiv 2 \pmod{7}$?

let $m = 3 \cdot 5 \cdot 7 = 105$,
$M1 = m/3 = 35$, $M2 = m/5 = 21$, and $M3 = m/7 = 15$.
We see that 2 is an inverse of $M1 = 35$ modulo 3,
because $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod 3$;
1 is an inverse of $M2 = 21$ modulo 5, because $21 \equiv 1 \pmod 5$;
1 is an inverse of $M3 = 15 \pmod 7$, because $15 \equiv 1 \pmod 7$.
The solutions to this system are those x such that
$x \equiv a1M1y1 + a2M2y2 + a3M3y3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}$.
23 is the smallest positive integer that is a simultaneous solution that leaves a remainder of 2 when divided by 3, a remainder of 3 when divided by 5, and a remainder of 2 when divided by 7.

An Application of Primes!

- When you visit a secure web site (https:… address, indicated by padlock icon in IE, key icon in Netscape), the browser and web site may be using a technology called *RSA encryption*.
- This *public-key cryptography* scheme involves exchanging *public keys* containing the product *pq* of two random large primes *p* and *q* (a *private key*) which must be kept secret by a given party.
- So, the security of your day-to-day web transactions depends critically on the fact that all known factoring algorithms are intractable!

Public Key Cryptography

- In ***private key cryptosystems***, the same secret "key" string is used to both encode and decode messages.
  - This raises the problem of how to securely communicate the key strings.
- In ***public key cryptosystems***, there are two *complementary* keys instead.
  - One key decrypts the messages that the other one encrypts.
- This means that one key (the *public key*) can be made public, while the other (the *private key*) can be kept secret from everyone.
  - Messages to the owner can be encrypted by anyone using the public key, but can *only* be decrypted by the owner using the private key.
    - Like having a private lock-box with a slot for messages.
  - Or, the owner can encrypt a message with their private key, and then anyone can decrypt it, and know that *only* the owner could have encrypted it.
    - This is the basis of digital signature systems.
- The most famous public-key cryptosystem is RSA.
  - It is based entirely on number theory!

Rivest-Shamir-Adleman(RSA)

- Choose a pair p, q of large random prime numbers with about the same number of bits
  - Let $n = pq$
- Choose exponent e that is relatively prime to $(p-1)(q-1)$ and $1 < e < (p-1)(q-1)$
- Compute d, the inverse of e modulo $(p-1)(q-1)$.

- The **public key** consists of: n, and e.
- The **private key** consists of: n, and d.

RSA Encryption

- To encrypt a message encoded as an integer:
  - Translate each letter into an integer and group them to form larger integers, each representing a block of letters. Each block is encrypted using the mapping

$$C = M^e \bmod n.$$

- Example: RSA encryption of the message **STOP** with $p = 43$, $q = 59$, and $e = 13$
  - $n = 43 \times 59 = 2537$
  - $\gcd(e, (p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$
  - **STOP** -> 1819 1415
  - 1819^{13} **mod** 2537 = 2081; 1415^{13} **mod** 2537 = 2182
  - Encrypted message: **2081 2182**

RSA Decryption

- To decrypt the encoded message C,
  - Compute $M = C^d \bmod n$
  - Recall that d is an inverse of e modulo $(p-1)(q-1)$.

- Example: RSA decryption of the message **0981 0461** encrypted with $p = 43$, $q = 59$, and $e = 13$
  - $n = 43 \times 59 = 2537$; $d = 937$
  - 0981^{937} **mod** $2537 = 0704$
  - 0461^{937} **mod** $2537 = 1115$
  - Decrypted message: **0704 1115**
  - Translation back to English letters: **HELP**

Computer Arithmetic with Large Integers

- By Chinese Remainder Theorem, an integer *a* where $0 \le a < m = \prod m_i$, $\gcd(m_i, m_{j \ne i}) = 1$, can be represented by *a*'s residues mod m_i: (a mod m_1, a mod m_2, …, a mod m_n)

each m_i is an integer greater than 2, gcd*(mi,mj) = 1 whenever i != j ,* $m = m_1 m_2 \ldots m_n$ *is greater* than the results of the arithmetic operations.

- To perform arithmetic with large integers represented in this way,
  - Simply perform operations on the separate residues!
    - Each of these might be done in a single machine operation.
    - The operations may be easily parallelized on a vector machine.
  - Works so long as m > the desired result.

Computer Arithmetic Example

- For example, the following numbers are relatively prime:
  $m_1 = 2^{25}-1 = 33{,}554{,}431 = 31 \cdot 601 \cdot 1{,}801$
  $m_2 = 2^{27}-1 = 134{,}217{,}727 = 7 \cdot 73 \cdot 262{,}657$
  $m_3 = 2^{28}-1 = 268{,}435{,}455 = 3 \cdot 5 \cdot 29 \cdot 43 \cdot 113 \cdot 127$
  $m_4 = 2^{29}-1 = 536{,}870{,}911 = 233 \cdot 1{,}103 \cdot 2{,}089$
  $m_5 = 2^{31}-1 = 2{,}147{,}483{,}647$ (prime)
- Thus, we can uniquely represent all numbers up to $m = \prod m_i \approx 1.4\times10^{42} \approx 2^{139.5}$ by their residues r_i modulo these five m_i.
  - *E.g.,* 10^{30} = (r_1 = 20,900,945; r_2 = 18,304,504; r_3 = 65,829,085; r_4 = 516,865,185; r_5 = 1,234,980,730)
- To add two such numbers in this representation,
  - Just add the residues using machine-native 32-bit integers.
  - Take the result mod 2^k-1:
    - If result is ≥ the appropriate 2^k-1 value, subtract out 2^k-1
      - or just take the low k bits and add 1.
  - Note: No carries are needed between the different pieces!

Pseudoprimes

- Ancient Chinese mathematicians noticed that whenever n is prime, $2^{n-1} \equiv 1 \pmod{n}$.
  - Some also claimed that the converse was true.
- However, it turns out that the converse is not true!
  - If $2^{n-1} \equiv 1 \pmod{n}$, it doesn't follow that n is prime.
    - For example, $341 = 11 \cdot 31$, but $2^{340} \equiv 1 \pmod{341}$.
- Composites n with this property are called ***pseudoprimes***.
  - More generally, if $b^{n-1} \equiv 1 \pmod{n}$ and n is composite, then n is called a *pseudoprime to the base b*.

Carmichael Numbers

- These are sort of the "ultimate pseudoprimes."
- A *Carmichael number* is a composite n such that $b^{n-1} \equiv 1 \pmod{n}$ for all b relatively prime to n.
- The smallest few are 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341.

Fermat's Little Theorem

- Fermat generalized the ancient observation that $2^{p-1} \equiv 1 \pmod{p}$ for primes p to the following more general theorem:
- **Theorem:** (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 $a^p \equiv a \pmod{p}$.
- Example (Exponentiation MOD a Prime)
  - Find $2^{301} \bmod 5$: By FLT, $2^4 \equiv 1 \pmod 5$. Hence,

    $2^{300} = (2^4)^{75} \equiv 1 \pmod 5$.

    Therefore, $2^{301} = (2^{300}) \cdot 2 \equiv 1 \cdot 2 \pmod 5 \equiv 2 \pmod 5$