

Monotonic Functions

■ Definition: Let A and B be subsets of R, the set of real numbers. A function $f: A \rightarrow B$ is *strictly increasing* if

 $\forall x {\in} A \ \forall y {\in} A \ x {<} y \ {\rightarrow} \ f(x) {<} f(y).$

- $f: A \to B$ is strictly decreasing if $\forall x \in A \ \forall y \in A \ x < y \ \to f(x) > f(y)$.
- Note that strictly increasing, or strictly decreasing (*strictly monotone*) functions have to be one-to-one.

5

Inverse Function

Definition: Let function *f*: A → B be a bijection.
 The *inverse function* of *f*, denoted *f*⁻¹, is the function,

 $f^{-1}: B \to A$, that assigns to each element b of B the element a of A such that f(a) = b.

- □ *f* is called *invertible*.



278

Inverse Function...

- Example: Let $f: \mathbb{Z} \to \mathbb{Z}$, where f(x) = x + 1.
 - \Box *f* is a bijection; what is f^{-1} ?
 - □ Suppose f(x) = y; then x + 1 = y; so $x = y 1 = f^{-1}(y)$ $f^{-1}(x) = x - 1$.

S

Identity Function

- Let *A* be a set. The *identity function* on *A* is the function $\iota_A : A \to A$, where $\forall x \in A \iota_A(x) = x$.
- Notes:

5

- $\ \ \ \ \ \iota_A$ assigns each element of A to itself.
- $\ \square \ \iota_A$ is a bijection.

Characteristic and Constant Functions

- Let A be a set. The characteristic function
 f: A → {0, 1}, maps each element of A to either 0
 or 1
- Let A be a set. The constant function
 f: A → {t} maps each element of A to the same

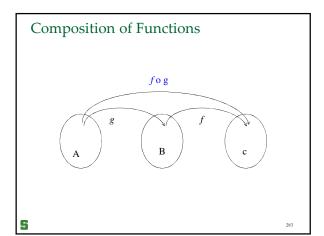
281

Compositions of Functions

Definition: Let g be a function from A to B and f
a function from B to C, that is,

$$g: A \to B$$
 $f: B \to C$

■ The *composition* of f and g, denoted f o g, is function from A to C, defined as follows $\forall x \in A \ (f \circ g)(x) = f(g(x)).$



Example

Consider the two functions

g: **Z** → **Z**, where
$$g(x) = 3x + 2$$
.
 $f: \mathbf{Z} \to \mathbf{Z}$, where $f(x) = 2x + 3$

- What are $f \circ g$, and $g \circ f$?
- □ $f \circ g: \mathbb{Z} \to \mathbb{Z}$, where $(f \circ g)(x) = f(g(x)) = f(3x + 2) = 2(3x + 2) + 3$ = 6x + 7
- □ $g \circ f: Z \to Z$, where $(g \circ f)(x) = g(f(x)) = g(2x+3) = 3(2x+3) + 2$ = 6x + 11

284

Example

Consider the following $R \to R$ functions:

$$f(x) = x^3 - 4x$$
 $g(x) = \frac{1}{x^2 + 1}$ $h(x) = x^4$

Compute the following:

- 1. $f \circ f$
- 5. $f \circ h$
- 2. $f \circ g$
- 6. $f \circ (h \circ g)$
- 3. $g \circ f$
- 7. $(f \circ h) \circ g$
- 4. $h \circ g$

S

Example

5

Consider the following $R \to R$ functions:

$$f(x) = x^3 - 4x$$
 $g(x) = \frac{1}{x^2 + 1}$ $h(x) = x^4$

Compute the following:

- 1. $f \circ f = f(x^3 4x) = (x^3 4x)^3 4(x^3 4x)$
- 2. $f \circ g = f(g(x)) = f\left(\frac{1}{x^2 + 1}\right) = \left(\frac{1}{x^2 + 1}\right)^3 4\left(\frac{1}{x^2 + 1}\right) = \frac{1 4(x^2 + 1)^3}{(x^2 + 1)^3}$
- 3. $g \circ f = g(f(x)) = g(x^3 4x) = \frac{1}{(x^3 4x)^2 + 1}$

Note that $f \circ g \neq g \circ f$

S

Example....

Recall that $f(x) = x^3 - 4x$ $g(x) = \frac{1}{x^2 + 1}$ $h(x) = x^4$

4.
$$h \circ g = h(g(x)) = \left(\frac{1}{x^2 + 1}\right)^4$$
 5. $f \circ h = f(x^4) = \left((x^4)\right)^3 - 4(x^4)$

6.
$$f \circ (h \circ g) = f\left(\left(\frac{1}{x^2 + 1}\right)^4\right) = \left(\left(\frac{1}{x^2 + 1}\right)^4\right)^3 - 4\left(\left(\frac{1}{x^2 + 1}\right)^4\right)$$

7.
$$(f \circ h) \circ g = \left(\left(\frac{1}{x^2 + 1} \right)^4 \right)^3 - 4 \left(\left(\frac{1}{x^2 + 1} \right)^4 \right)$$

Note that at least for this example we have $f \circ (h \circ g) = (f \circ h) \circ g$

In fact, the above is true always.

5

Graph of a Function

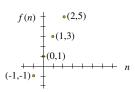
■ Definition: Let $f: A \rightarrow B$. The *graph* of f is the set of ordered pairs

$$G_f = \{(x, f(x)) \mid x \in A\}.$$

288

Graph of a Function....

■ The graph of the function $f: \mathbb{Z} \to \mathbb{Z}$, where f(n) = 2n + 1, is $G_f = \{(n, 2n + 1) \mid n \in \mathbb{Z}\}$



5

Important Integer Functions

- Whole numbers constitute the backbone of discrete mathematics. We often need to convert fractions or arbitrary real numbers to integers. These integer functions will help us do that.
- Besides the identity function, some important functions are:
 - □ The *floor* function,
 - □ The *ceiling* function,
 - □ The *mod* function.

Floor Function

Definition: The *floor function* from *R* to *Z* assigns to the real number *x*, the largest integer ≤ *x*.

The value of the floor function at x is denoted by $\lfloor x \rfloor$.

- Examples:
 - □ | 18 | **=** 18
 - □ [3.75] = 3
 - □ [-4.5]=-5

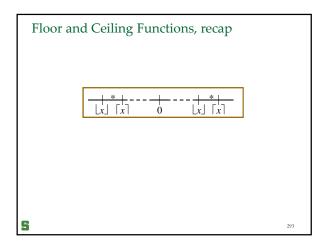
S

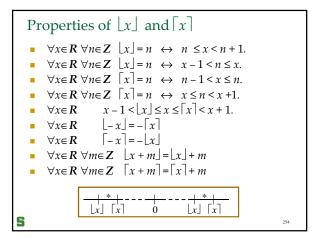
Ceiling Function

- The *ceiling function* from R to Z assigns to the real number x the smallest integer $\geq x$. The value of the ceiling function at x is denoted by $\lceil x \rceil$.
- Examples:

5

- □ [18]=18
- □ [3.75] = 4
- □ [-4.5]=-4





Example

Prove or disprove the following statements about real numbers:

a) $\lceil \lfloor x \rfloor \rceil = \lfloor x \rfloor$ b) $\lfloor 2x \rfloor = 2 \lfloor x \rfloor$ c) $\lceil x \rceil + \lceil y \rceil - \lceil x + y \rceil \in \{0, 1\}$ d) $\lceil xy \rceil = \lceil x \rceil \lceil y \rceil$ e) $\lceil \frac{x}{2} \rceil = \lceil \frac{x+1}{2} \rceil$

Example: Solution

Prove or disprove the following statements about real numbers:

a) $\lceil \lfloor x \rfloor \rceil = \lfloor x \rfloor$ Answer: True

b) $\lfloor 2x \rfloor = 2 \lfloor x \rfloor$ Answer: False, try $x = \frac{1}{2}$ c) $\lceil x \rceil + \lceil y \rceil - \lceil x + y \rceil \in \{0,1\}$ Answer: True

d) $\lceil xy \rceil = \lceil x \rceil \lceil y \rceil$ Answer: Fasle, try $x = \frac{1}{4}$, y = 3e) $\left\lceil \frac{x}{2} \right\rceil = \left\lceil \frac{x+1}{2} \right\rceil$ Answer: Fasle, try x = 4

Division

Which relation defines *dividing* 101 by 11?

101 = 11 × 8 + 13

101 = 11 × 11 - 20

101 = 11 × 9 + 2

Division... Let n be an integer and m a positive integer. Then there are *unique* integers q and r, with $0 \le r < m$, such that n = mq + r \square *n* is called the *dividend* \square *m* is called the *divisor* □ *q* is called the *quotient* \Box *r* is called the *remainder* Examples: $101 = 11 \times 9 + 2$ How about: $101 = 11 \times 8 + 13$ Examples: -11 = 3(-4) + 1How about: -11 = 3(-3) - 2Remainder cannot be a negative number

The mod Function

- When dividing an integer n by a number m, the quotient of the division is ⌊n/m⌋. What about a simple notation for the remainder of this division?
- That's what the mod function is about:
- $n \mod m$
- m is called modulus
- $n = m \times \lfloor n/m \rfloor + (n \mod m)$ quotient remainder

5

Example

■ Formally, the *mod* function is a mapping: $mod : \mathbb{Z} \times \mathbb{Z}^+ \to N$ where

$$n \mod m = n - m \times \lfloor n/m \rfloor$$

Examples:

```
5 \mod 3 = 5 - (3 \times \lfloor 5/3 \rfloor) = 5 - (3 \times \lfloor 1.6 \rfloor) = 5 - (3 \times 1) = 2
```

30

Example

- $n \bmod m = n (m \times \lfloor n/m \rfloor)$
- Examples:

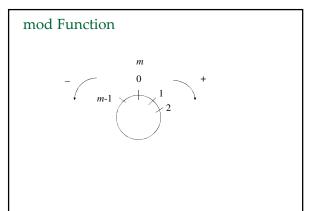
-5 mod 3 = -5 - (3 ×
$$\lfloor$$
-5/3 \rfloor)
= -5 - (3 × \lfloor -1.6 \rfloor) = -5 - (3 × (-2)) = 1.

We also write:

 $5 \equiv 2 \mod 3,$
 $9 \equiv 0 \mod 3,$

 $-5 \equiv 1 \bmod 3.$

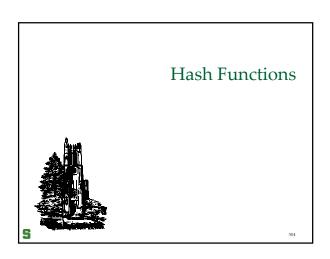
501



List Search Methods

- Problem: Given a *list* of elements, how fast can we decide whether or not a given input element belongs to the list?
 - Linear search
 - Binary search; need to sort the list first
 - Hash table

5



Hash Functions

- A hash function h: keys → integers maps "keys" to "small" integers (buckets)
- Ideal features:
 - □ The function should be easy to compute
 - □ The range values should be "evenly" distributed
 - Given an image, it should not be "easy" to find its preimage
- Applications
 - Searching/indexing
 - Information hiding
 - □ File signature

5

305

Hashing for Indexing

- A hash function h: keys → integers maps "keys" to "small" integers (buckets)
- Ideally this mapping is done in a "random" manner so that the bucket values are evenly distributed despite irregularities in the keys.
- For simplicity, we will assume that the keys are also integers, denoted by *k*, and the number of buckets is demoted by *m*. Note that the buckets are indexed 0 through *m* 1.

Simple Hash Functions

- $h(k) = k \bmod m$
- Suggestion: Choose m to be a prime number that isn't close to a power of 2.
- $h(k) = k(k+3) \bmod m$