

## Basic Prerequisite Mathematics

### SET THEORY

#### Common Sets

- $\mathbb{N} = \{0, 1, 2, \dots\}$ : the natural numbers, or non-negative integers. The convention in computer science is to include 0 in the natural numbers.
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ : the integers
- $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$ : the positive integers
- $\mathbb{Z}^- = \{-1, -2, -3, \dots\}$ : the negative integers
- $\mathbb{Q}$  the rational numbers,  $\mathbb{Q}^+$  the positive rationals, and  $\mathbb{Q}^-$  the negative rationals.
- $\mathbb{R}$  the real numbers,  $\mathbb{R}^+$  the positive reals, and  $\mathbb{R}^-$  the negative reals.

#### Notation

For any sets  $A$  and  $B$ , we will use the following standard notation.

- $x \in A$ : “ $x$  is an element of  $A$ ” or “ $A$  contains  $x$ ”
- $A \subseteq B$ : “ $A$  is a subset of  $B$ ” or “ $A$  is included in  $B$ ”
- $A = B$ : “ $A$  equals  $B$ ” (Note that  $A = B$  if and only if  $A \subseteq B$  and  $B \subseteq A$ .)
- $A \subsetneq B$ : “ $A$  is a proper subset of  $B$ ”  
(Note that  $A \subsetneq B$  if and only if  $A \subseteq B$  and  $A \neq B$ .)
- $A \cup B$ : “ $A$  union  $B$ ”
- $A \cap B$ : “ $A$  intersection  $B$ ”
- $A - B$ : “ $A$  minus  $B$ ” (*set* difference)
- $|A|$ : “cardinality of  $A$ ” (the number of elements of  $A$ )
- $\emptyset$  or  $\{\}$ : “the empty set”
- $\mathcal{P}(A)$  or  $2^A$ : “powerset of  $A$ ” (the set of all subsets of  $A$ )  
If  $A = \{a, 34, \triangle\}$ , then  $\mathcal{P}(A) = \{\{\}, \{a\}, \{34\}, \{\triangle\}, \{a, 34\}, \{a, \triangle\}, \{34, \triangle\}, \{a, 34, \triangle\}\}$ .  
 $S \in \mathcal{P}(A)$  means the same as  $S \subseteq A$ .
- $\{x \in A \mid P(x)\}$ : “the set of elements  $x$  in  $A$  for which  $P(x)$  is true”  
For example,  $\{x \in \mathbb{Z} \mid \cos(\pi x) > 0\}$  represents the set of integers  $x$  for which  $\cos(\pi x)$  is greater than zero, *i.e.*, it is equal to  $\{\dots, -4, -2, 0, 2, 4, \dots\} = \{x \in \mathbb{Z} \mid x \text{ is even}\}$ .

- $A \times B$ : “the cross product or Cartesian product of  $A$  and  $B$ ”  
 $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$ .  
 If  $A = \{1, 2, 3\}$  and  $B = \{5, 6\}$ , then  $A \times B = \{(1, 5), (1, 6), (2, 5), (2, 6), (3, 5), (3, 6)\}$ .
- $A^n$ : “the cross product of  $n$  copies of  $A$ ”  
 This is set of all sequences of  $n \geq 1$  elements, each of which is in  $A$ .
- $B^A$  or  $A \rightarrow B$ : “the set of all functions from  $A$  to  $B$ .”
- $f : A \rightarrow B$  or  $f \in B^A$ : “ $f$  is a function from  $A$  to  $B$ ”  
 $f$  associates one element  $f(x) \in B$  to every element  $x \in A$ .

## NUMBER THEORY

For any two natural numbers  $a$  and  $b$ , we say that  $a$  *divides*  $b$  if there exists a natural number  $c$  such that  $b = ac$ . In such a case, we say that  $a$  is a *divisor* of  $b$  (e.g., 3 is a divisor of 12 but 3 is not a divisor of 16). Note that any natural number is a divisor of 0 and 1 is a divisor of any natural number. A number  $a$  is *even* if 2 divides  $a$  and is *odd* if 2 does not divide  $a$ .

A natural number  $p$  is *prime* if it has exactly two positive divisors (e.g., 2 is prime since its positive divisors are 1 and 2 but 1 is **not** prime since it only has one positive divisor: 1). There are an infinite number of prime numbers and any integer greater than one can be expressed in a unique way as a finite product of prime numbers (e.g.,  $8 = 2^3$ ,  $77 = 7 \times 11$ ,  $3 = 3$ ).

## Inequalities

For any integers  $m$  and  $n$ ,  $m < n$  if and only if  $m + 1 \leq n$  and  $m > n$  if and only if  $m \geq n + 1$ . For any real numbers  $w$ ,  $x$ ,  $y$ , and  $z$ , the following properties always hold (they also hold when  $<$  and  $\leq$  are exchanged throughout with  $>$  and  $\geq$ , respectively).

- if  $x < y$  and  $w \leq z$ , then  $x + w < y + z$
- if  $x < y$ , then 
$$\begin{cases} xz < yz & \text{if } z > 0 \\ xz = yz & \text{if } z = 0 \\ xz > yz & \text{if } z < 0 \end{cases}$$
- if  $x \leq y$  and  $y < z$  (or if  $x < y$  and  $y \leq z$ ), then  $x < z$

## Functions

Here are some common number-theoretic functions together with their definitions and properties of them. (Unless noted otherwise, in this section,  $x$  and  $y$  represent arbitrary real numbers and  $k$ ,  $m$ , and  $n$  represent arbitrary positive integers.)

- $\min\{x, y\}$ : “minimum of  $x$  and  $y$ ” (the smallest of  $x$  or  $y$ )  
 Properties:  $\min\{x, y\} \leq x$   
 $\min\{x, y\} \leq y$

- $\max\{x, y\}$ : “maximum of  $x$  and  $y$ ” (the largest of  $x$  or  $y$ )  
 Properties:  $x \leq \max\{x, y\}$   
 $y \leq \max\{x, y\}$
- $\lfloor x \rfloor$ : “floor of  $x$ ” (the greatest integer less than or equal to  $x$ , *e.g.*,  $\lfloor 5.67 \rfloor = 5$ ,  $\lfloor -2.01 \rfloor = -3$ )  
 Properties:  $x - 1 < \lfloor x \rfloor \leq x$   
 $\lfloor -x \rfloor = -\lceil x \rceil$   
 $\lfloor x + k \rfloor = \lfloor x \rfloor + k$   
 $\lfloor \lfloor k/m \rfloor / n \rfloor = \lfloor k/mn \rfloor$   
 $(k - m + 1)/m \leq \lfloor k/m \rfloor$
- $\lceil x \rceil$ : “ceiling of  $x$ ” (the least integer greater than or equal to  $x$ , *e.g.*,  $\lceil 5.67 \rceil = 6$ ,  $\lceil -2.01 \rceil = -2$ )  
 Properties:  $x \leq \lceil x \rceil < x + 1$   
 $\lceil -x \rceil = -\lfloor x \rfloor$   
 $\lceil x + k \rceil = \lceil x \rceil + k$   
 $\lceil \lceil k/m \rceil / n \rceil = \lceil k/mn \rceil$   
 $\lceil k/m \rceil \leq (k + m - 1)/m$   
 Additional property of  $\lfloor \cdot \rfloor$  and  $\lceil \cdot \rceil$ :  $\lfloor k/2 \rfloor + \lceil k/2 \rceil = k$ .
- $|x|$ : “absolute value of  $x$ ” ( $|x| = x$  if  $x \geq 0$ ;  $-x$  if  $x < 0$ , *e.g.*,  $|5.67| = 5.67$ ,  $|-2.01| = 2.01$ )  
 BEWARE! The same notation is used to represent the cardinality  $|A|$  of a set  $A$  and the absolute value  $|x|$  of a number  $x$  so be sure you are aware of the context in which it is used.
- $m \operatorname{div} n$ : “the quotient of  $m$  divided by  $n$ ” (integer division of  $m$  by  $n$ , *e.g.*,  $5 \operatorname{div} 6 = 0$ ,  $27 \operatorname{div} 4 = 6$ ,  $-27 \operatorname{div} 4 = -6$ )  
 Properties: If  $m, n > 0$ , then  $m \operatorname{div} n = \lfloor m/n \rfloor$   
 $(-m) \operatorname{div} n = -(m \operatorname{div} n) = m \operatorname{div} (-n)$
- $m \operatorname{rem} n$ : “the remainder of  $m$  divided by  $n$ ” (*e.g.*,  $5 \operatorname{rem} 6 = 5$ ,  $27 \operatorname{rem} 4 = 3$ ,  $-27 \operatorname{rem} 4 = -3$ )  
 Properties:  $m = (m \operatorname{div} n) \cdot n + m \operatorname{rem} n$   
 $(-m) \operatorname{rem} n = -(m \operatorname{rem} n) = m \operatorname{rem} (-n)$
- $m \bmod n$ : “ $m$  modulo  $n$ ” (*e.g.*,  $5 \bmod 6 = 5$ ,  $27 \bmod 4 = 3$ ,  $-27 \bmod 4 = 1$ )  
 Properties:  $0 \leq m \bmod n < n$   
 $n$  divides  $m - (m \bmod n)$ .
- $\gcd(m, n)$ : “greatest common divisor of  $m$  and  $n$ ” (the largest positive integer that divides both  $m$  and  $n$ )  
 For example,  $\gcd(3, 4) = 1$ ,  $\gcd(12, 20) = 4$ ,  $\gcd(3, 6) = 3$
- $\operatorname{lcm}(m, n)$ : “least common multiple of  $m$  and  $n$ ” (the smallest positive integer that  $m$  and  $n$  both divide)  
 For example,  $\operatorname{lcm}(3, 4) = 12$ ,  $\operatorname{lcm}(12, 20) = 60$ ,  $\operatorname{lcm}(3, 6) = 6$   
 Properties:  $\gcd(m, n) \cdot \operatorname{lcm}(m, n) = m \cdot n$ .

# CALCULUS

## Limits and Sums

An infinite sequence of real numbers  $\{a_n\} = a_1, a_2, \dots, a_n, \dots$  *converges* to a limit  $L \in \mathbb{R}$  if, for every  $\varepsilon > 0$ , there exists  $n_0 \geq 0$  such that  $|a_n - L| < \varepsilon$  for every  $n \geq n_0$ . In this case, we write  $\lim_{n \rightarrow \infty} a_n = L$ . Otherwise, we say that the sequence *diverges*.

If  $\{a_n\}$  and  $\{b_n\}$  are two sequences of real numbers such that  $\lim_{n \rightarrow \infty} a_n = L_1$  and  $\lim_{n \rightarrow \infty} b_n = L_2$ , then

$$\lim_{n \rightarrow \infty} (a_n + b_n) = L_1 + L_2 \quad \text{and} \quad \lim_{n \rightarrow \infty} (a_n \cdot b_n) = L_1 \cdot L_2.$$

In particular, if  $c$  is any real number, then

$$\lim_{n \rightarrow \infty} (c \cdot a_n) = c \cdot L_1.$$

The sum  $a_1 + a_2 + \dots + a_n$  and product  $a_1 \cdot a_2 \cdot \dots \cdot a_n$  of the finite sequence  $a_1, a_2, \dots, a_n$  are denoted by

$$\sum_{i=1}^n a_i \quad \text{and} \quad \prod_{i=1}^n a_i.$$

If the elements of the sequence are all different and  $S = \{a_1, a_2, \dots, a_n\}$  is the set of elements in the sequence, these can also be denoted by

$$\sum_{a \in S} a \quad \text{and} \quad \prod_{a \in S} a.$$

### Examples:

- For any  $a \in \mathbb{R}$  such that  $-1 < a < 1$ ,  $\lim_{n \rightarrow \infty} a^n = 0$ .
- For any  $a \in \mathbb{R}^+$ ,  $\lim_{n \rightarrow \infty} a^{1/n} = 1$ .
- For any  $a \in \mathbb{R}^+$ ,  $\lim_{n \rightarrow \infty} (1/n)^a = 0$ .
- $\lim_{n \rightarrow \infty} (1 + 1/n)^n = e = 2.71828182845904523536 \dots$

- For any  $a, b \in \mathbb{R}$ , the *arithmetic* sum is given by:

$$\sum_{i=0}^n (a + ib) = (a) + (a + b) + (a + 2b) + \dots + (a + nb) = \frac{1}{2}(n+1)(2a + nb).$$

- For any  $a, b \in \mathbb{R}^+$ , the *geometric* sum is given by:

$$\sum_{i=0}^n (ab^i) = a + ab + ab^2 + \dots + ab^n = \frac{a(1 - b^{n+1})}{1 - b}.$$

## EXPONENTS AND LOGARITHMS

**Definition:** For any  $a, b, c \in \mathbb{R}^+$ ,  $a = \log_b c$  if and only if  $b^a = c$ .

**Notation:** For any  $x \in \mathbb{R}^+$ ,  $\ln x = \log_e x$  and  $\lg x = \log_2 x$ .

For any  $a, b, c \in \mathbb{R}^+$  and any  $n \in \mathbb{Z}^+$ , the following properties always hold.

- $\sqrt[n]{b} = b^{1/n}$
- $b^a b^c = b^{a+c}$
- $(b^a)^c = b^{ac}$
- $b^a / b^c = b^{a-c}$
- $b^0 = 1$
- $a^b c^b = (ac)^b$
- $b^{\log_b a} = a = \log_b b^a$
- $a^{\log_b c} = c^{\log_b a}$
- $\log_b(ac) = \log_b a + \log_b c$
- $\log_b(a^c) = c \cdot \log_b a$
- $\log_b(a/c) = \log_b a - \log_b c$
- $\log_b 1 = 0$
- $\log_b a = \log_c a / \log_c b$

## BINARY NOTATION

A *binary number* is a sequence of bits  $a_k \cdots a_1 a_0$  where each bit  $a_i$  is equal to 0 or 1. Every binary number represents a natural number in the following way:

$$(a_k \cdots a_1 a_0)_2 = \sum_{i=0}^k a_i 2^i = a_k 2^k + \cdots + a_1 2 + a_0.$$

For example,  $(1001)_2 = 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 8 + 1 = 9$ ,  $(01110)_2 = 8 + 4 + 2 = 14$ .

### Properties:

- If  $a = (a_k \cdots a_1 a_0)_2$ , then  $2a = (a_k \cdots a_1 a_0 0)_2$ , *e.g.*,  $9 = (1001)_2$  so  $18 = (10010)_2$ .
- If  $a = (a_k \cdots a_1 a_0)_2$ , then  $\lfloor a/2 \rfloor = (a_k \cdots a_1)_2$ , *e.g.*,  $9 = (1001)_2$  so  $4 = (100)_2$ .
- The smallest number of bits required to represent the positive integer  $n$  in binary is called the *length* of  $n$  and is equal to  $\lceil \log_2(n+1) \rceil$ .

Make sure you know how to add and multiply two binary numbers. For example,  $(1111)_2 + (101)_2 = (10100)_2$  and  $(1111)_2 \times (101)_2 = (1001011)_2$ .