Useful Rules for Big-O

For any **polynomial** $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, where $a_0, a_1, \ldots, a_n$ are real numbers, $f(x)$ is $O(x^n)$.

If $f_1(x)$ is $O(g(x))$ and $f_2(x)$ is $O(g(x))$, then $(f_1 + f_2)(x)$ is $O(g(x))$.

If $f_1(x)$ is $O(g_1(x))$ and $f_2(x)$ is $O(g_2(x))$, then $(f_1 + f_2)(x)$ is $O(\max(g_1(x), g_2(x)))$

If $f_1(x)$ is $O(g_1(x))$ and $f_2(x)$ is $O(g_2(x))$, then $(f_1 f_2)(x)$ is $O(g_1(x)\, g_2(x))$.

Complexity Examples

What does the following algorithm compute?

procedure who_knows($a_1, a_2, \ldots, a_n$: integers)
who_knows := 0
for i := 1 to n-1
  for j := i+1 to n
    if $|a_i - a_j| >$ who_knows **then** who_knows := $|a_i - a_j|$
{who_knows is the maximum difference between any two numbers in the input sequence}

Comparisons: n-1 + n-2 + n-3 + … + 1
$= (n - 1)n/2 = 0.5n^2 - 0.5n$

Time complexity is $O(n^2)$.

Complexity Examples

Another algorithm solving the same problem:

procedure max_diff($a_1, a_2, \ldots, a_n$: integers)
min := a_1
max := a_1
for i := 2 to n
    if $a_i <$ min **then** min := a_i
    else if $a_i >$ max **then** max := a_i
max_diff := max - min

Comparisons (worst case): 2n - 2

Time complexity is O(n).

Division

If a and b are integers with $a \neq 0$, we say that a **divides** b if there is an integer c so that $b = ac$.

When a divides b we say that a is a **factor** of b and that b is a **multiple** of a.

The notation **a | b** means that a divides b.

We write **a X b** when a does not divide b.
(see book for correct symbol).

Divisibility Theorems

For integers a, b, and c it is true that

- if a | b and a | c, then a | (b + c)
  Example: 3 | 6 and 3 | 9, so 3 | 15.
- if a | b, then a | bc for all integers c
  Example: 5 | 10, so 5 | 20, 5 | 30, 5 | 40, …
- if a | b and b | c, then a | c
  Example: 4 | 8 and 8 | 24, so 4 | 24.

Primes

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.

The fundamental theorem of arithmetic:

Every positive integer can be written **uniquely** as the **product of primes**, where the prime factors are written in order of increasing size.

Primes

Examples:

15 = $3 \cdot 5$

48 = $2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3$

17 = 17

100 = $2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$

512 = $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^9$

515 = $5 \cdot 103$

28 = $2 \cdot 2 \cdot 7 = 2^2 \cdot 7$

Primes

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

This is easy to see: if n is a composite integer, it must have two divisors p_1 and p_2 such that $p_1 \cdot p_2 = n$ and $p_1 \geq 2$ and $p_2 \geq 2$.

p_1 and p_2 cannot both be greater than $\sqrt{n}$, because then $p_1 \cdot p_2$ would be greater than n.

If the smaller number of p_1 and p_2 is not a prime itself, then it can be broken up into prime factors that are smaller than itself but ≥ 2.

The Division Algorithm

Let **a** be an integer and **d** a positive integer. Then there are unique integers **q** and **r**, with **$0 \leq r < d$**, such that **$a = dq + r$**.

In the above equation,
- **d** is called the divisor,
- **a** is called the dividend,
- **q** is called the quotient, and
- **r** is called the remainder.

The Division Algorithm

Example:

When we divide 17 by 5, we have

$17 = 5 \cdot 3 + 2$.

- 17 is the dividend,
- 5 is the divisor,
- 3 is called the quotient, and
- 2 is called the remainder.

The Division Algorithm

Another example:

What happens when we divide -11 by 3 ?

Note that the remainder cannot be negative.

$-11 = 3 \cdot (-4) + 1$.

- -11 is the dividend,
- 3 is the divisor,
- -4 is called the quotient, and
- 1 is called the remainder.

Greatest Common Divisors

Let a and b be integers, not both zero.
The largest integer d such that $d \mid a$ and $d \mid b$ is called the **greatest common divisor** of a and b.

The greatest common divisor of a and b is denoted by gcd(a, b).

Example 1: What is gcd(48, 72) ?

The positive common divisors of 48 and 72 are 1, 2, 3, 4, 6, 8, 12, 16, and 24, so gcd(48, 72) = 24.

Example 2: What is gcd(19, 72) ?

The only positive common divisor of 19 and 72 is 1, so gcd(19, 72) = 1.

Greatest Common Divisors

Using prime factorizations:

$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$,
where $p_1 < p_2 < \dots < p_n$ and $a_i, b_i \in \mathbf{N}$ for $1 \le i \le n$

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

Example:

$a = 60 = 2^2 3^1 5^1$

$b = 54 = 2^1 3^3 5^0$

$\gcd(a, b) = 2^1 3^1 5^0 = 6$

Relatively Prime Integers

Definition:

Two integers a and b are **relatively prime** if $\gcd(a, b) = 1$.

Examples:

Are 15 and 28 relatively prime?
Yes, $\gcd(15, 28) = 1$.
Are 55 and 28 relatively prime?
Yes, $\gcd(55, 28) = 1$.
Are 35 and 28 relatively prime?
No, $\gcd(35, 28) = 7$.

Relatively Prime Integers

Definition:

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

Examples:

Are 15, 17, and 27 pairwise relatively prime?
No, because $\gcd(15, 27) = 3$.

Are 15, 17, and 28 pairwise relatively prime?
Yes, because $\gcd(15, 17) = 1$, $\gcd(15, 28) = 1$ and $\gcd(17, 28) = 1$.

Least Common Multiples

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.

We denote the least common multiple of a and b by $\text{lcm}(a, b)$.

Examples:

$\text{lcm}(3, 7) = 21$

$\text{lcm}(4, 6) = 12$

$\text{lcm}(5, 10) = 10$

Least Common Multiples

Using prime factorizations:

$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$,
where $p_1 < p_2 < \dots < p_n$ and $a_i, b_i \in \mathbf{N}$ for $1 \le i \le n$

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

Example:

$a = 60 = 2^2 3^1 5^1$

$b = 54 = 2^1 3^3 5^0$

$\text{lcm}(a, b) = 2^2 3^3 5^1 = 4 \cdot 27 \cdot 5 = 540$

GCD and LCM

$a = 60 = 2^2 \cdot 3^1 \cdot 5^1$

$b = 54 = 2^1 \cdot 3^3 \cdot 5^0$

$\gcd(a, b) = 2^1 3^1 5^0 = 6$

$\text{lcm}(a, b) = 2^2 3^3 5^1 = 540$

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

Modular Arithmetic

Let a be an integer and m be a positive integer. We denote by **a mod m** the remainder when a is divided by m.

Examples:

9 mod 4 = 1

9 mod 3 = 0

9 mod 10 = 9

-13 mod 4 = 3

Congruences

Let a and b be integers and m be a positive integer. We say that **a is congruent to b modulo m** if m divides a – b.

We use the notation **$a \equiv b \pmod{m}$** to indicate that a is congruent to b modulo m.

In other words:
$a \equiv b \pmod{m}$ if and only if **a mod m = b mod m**.

Congruences

Examples:

Is it true that $46 \equiv 68 \pmod{11}$?
Yes, because 11 | (46 – 68).

Is it true that $46 \equiv 68 \pmod{22}$?
Yes, because 22 | (46 – 68).

For which integers z is it true that $z \equiv 12 \pmod{10}$?
It is true for any $z \in \{\ldots,-28, -18, -8, 2, 12, 22, 32, \ldots\}$

Theorem: 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.