A <u>set</u> is a well defined collection of objects. The objects are called the <u>elements</u> of the set.

Convention: Sets are denoted by capital letters $(A, B, S, T, \dots)$, elements by lower case letters $(a, b, x, y, \dots)$

If x is an element of a set A we write:

If y is not an element of a set A we write:

Two ways we will define a set:

① Writing elements between curly brackets

E.g.

② Using set-builder notation:

Common Sets:

Some basic sets of numbers we should be familiar with are:

- $\mathbb{Z} =$ the set of *integers* $= \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$,
- $\mathbb{N} =$ the set of *nonnegative integers* or *natural numbers* $= \{0, 1, 2, 3, \dots\} = \{x \in \mathbb{Z} \mid x \geq 0\}$,
- $\mathbb{Z}^+ =$ the set of *positive integers* $= \{1, 2, 3, \dots\} = \{x \in \mathbb{Z} \mid x > 0\}$,
- $\mathbb{Q} =$ the set of *rational numbers* $= \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z}, b \neq 0 \right\}$,
- $\mathbb{Q}^+ =$ the set of *positive rational numbers* $= \{x \in \mathbb{Q} \mid x > 0\}$,
- $\mathbb{R}$ is the set of *real numbers*.
- $[n] = \{1, 2, \dots, n\} =$ the set of integers from 1 to n, where $n \in \mathbb{Z}^+$. [1]

Let A and B be sets:

- If every element of A is an element of B we say A is a _____ of B:
- If and then .
- The set with no elements is the , denoted by or

Set Operations :

union : $A \cup B = \{x \mid x \in A \textbf{ or } x \in B\}$,

intersection: $A \cap B = \{x \mid x \in A \textbf{ and } x \in B\}$,

complement : $A^c = \overline{A} = \{x \mid x \notin A\}$,

difference : $A - B = \{x \mid x \in A \textbf{ and } x \notin B\} = A \cap B^c$

product : $A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}$.

Cardinality :

= number of elements in A

Laws of Set Theory :

1)	$(A^c)^c = A$	Law of Double Negation
2)	$(A \cup B)^c = A^c \cap B^c$ $(A \cap B)^c = A^c \cup B^c$	DeMorgan's Laws
3)	$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative Laws
4)	$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative Laws
5)	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive Laws
6)	$A \cup A = A$ $A \cap A = A$	Idempotent Laws
7)	$A \cup \emptyset = A$ $A \cap \mathscr{U} = A$	Identity Laws
8)	$A \cup A^c = \mathscr{U}$ $A \cap A^c = \emptyset$	Inverse Laws
9)	$A \cup \mathscr{U} = A$ $A \cap \emptyset = \emptyset$	Domination Laws
10)	$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorbtion Laws

Exercise :

Numbers 1, 2, 3, ..., 9 are written in a 3×3 array. The only permitted operations are to swap any two rows and or any two columns. Prove that it is impossible to attain the pattern on the right starting with the pattern on the left.

1	2	3
4	5	6
7	8	9

1	2	3
6	5	4
7	8	9

Appendix B : Properties of Integers

★ In this section all numbers are <u>integers</u> ★

a <u>divides</u> b (written $a \mid b$) if $b = ad$ for some integer d.

We say d is the **greatest common divisor** of a and b (written $\gcd(a,b)$) if and only if
(i) $d \mid a$ and $d \mid b$, and
(ii) if $c \mid a$ and $c \mid b$ then $c \le d$

Example :

a and b are if $\gcd(a,b) = 1$

Example:

Theorem B.1.1 — Division Algorithm. Let $a, b \in \mathbb{Z}$. Suppose that $b \neq 0$. Then there exist unique $q, r \in \mathbb{Z}$, with $0 \le r < |b|$ such that

$$a = qb + r.$$

We focus our attention on computing gcd's without factoring :

Lemma B.1.2 If $a = bq + r$ then $\gcd(a,b) = \gcd(b,r)$.

Example:

Theorem B.1.3 — Euclidean Algorithm. If a and b are positive integers, $b \neq 0$, and

$$\begin{aligned} a &= qb + r, \quad 0 \le r < b, \\ b &= q_1 r + r_1, \quad 0 \le r_1 < r, \\ r &= q_2 r_1 + r_2, \quad 0 \le r_2 < r_1, \\ &\vdots \qquad\qquad \vdots \\ r_k &= q_{k+2} r_{k+1} + r_{k+2}, \quad 0 \le r_{k+2} < r_{k+1}, \end{aligned}$$

then for k large enough, say $k = \ell$, we have $r_{\ell+1} = 0$, $r_{\ell-1} = q_{\ell+1} r_\ell$, and $\gcd(a,b) = r_\ell$.

Python B.1: Euclid's Algorithm for gcd in Python

```
def gcd(a,b):
    """Return the GCD of a and b using Euclid's Algorithm."""
    while b > 0:
        a, b = b, a%b
    return a
```

Extended Euclidean algorithm:

Example:

Theorem B.1.4 — Extended Euclidean Algorithm. If $\gcd(a,b) = d$ then there exist integers u and v such that

$$au + bv = d.$$

Primes :

A <u>prime</u> is an integer > 1 with exactly two positive divisors : 1 and itself.

Ex:

Lemma B.2.1 If p is a prime number and a and b are integers such that $p \mid ab$ then either $p \mid a$ or $p \mid b$.

Definition B.3.1 — Euler's ϕ-Function. For any positive integer n, $\phi(n)$ is the number of integers in $\{1, 2, \ldots, n\}$ which are relatively prime to n. In other words,

$$\phi(n) = |\{m \in \mathbb{Z} \mid 1 \leq m \leq n, \gcd(m,n) = 1\}|.$$

Theorem B.3.1 If n has prime factorization given by

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

then

$$\phi(n) = p_1^{e_1-1}(p_1 - 1)p_2^{e_2-1}(p_2 - 1) \cdots p_k^{e_k-1}(p_k - 1).$$

Modular Arithmetic:

Definition B.4.1 — a mod n. Let n be a fixed positive integer. For any integer a,

$$a \mod n \quad \text{(read } a \text{ modulo } n\text{)}$$

denotes the remainder upon dividing a by n. (Note: the *remainder* is an integer $0 \leq r < n$.)

Example:

Definition B.4.2 — Congruence. If a and b are integers and n is a positive integer, we write

$$a \equiv b \mod n$$

when n divides $a - b$. We say a is **congruent** to b modulo n.

Example:

Theorem B.4.1 — Modular Arithmetic.
If $a = c \mod n$ and $b = d \mod n$ then

- $(a+b) \equiv (c+d) \mod n$
- $a \cdot b \equiv c \cdot d \mod n$

Example: