Basic Properties of Integers

Notation: \( \mathbb{Z} \) : Set of integers

\[ \{ \ldots, -5, -4, -3, -2, -1, 0, 1, 2, \ldots \} \]

\[ \sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n \]

\[ \sum_{k=1}^{4} k^2 = 1^2 + 2^2 + 3^2 + 4^2 \]

\[ \sum_{j=0}^{5} 2^j = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 \]

- Arithmetic progression: A sequence \( \{a_n\}_{n \geq 0} \) such that \( a_{i+1} - a_i = \gamma, \forall i \geq 0 \).

In this case \( \gamma \) is called the Common difference.

- 1 \( \{1, 4, 7, 10, 13, \ldots \} \) 1 \rightarrow initial element
  3 : Common difference

- 2 \( \{2k + 5\}_{k \geq 1} = \{7, 9, 11, \ldots \} \)
  Common difference \( \gamma \)

\[ (2j + 5) - (2(j-1) + 5) = 2j + 5 - 2j + 2 - 5 = 2 \]
A sequence \( \{a_n\}_{n=1} \) is in geometric progression if \( a_{j+1} = d \cdot a_j \) for \( j \geq 1 \), \( d = "Common\ Ratio". \)

E.g. \( \{2, 6, 18, 54, 162, 486, \ldots\} \)

\( d = 3. \)

**Mathematical Induction:** Technique used often in proving a mathematical statement/formula/Theorem.

Two steps: (i) **Base step:** Consist of checking the statement/formula/Theorem for one specific value.
(ii) **Inductive step:** If \( S/F/T \) holds for a value \( n_0 \), then check that it also holds for \( n+1 \).

**Conclude:** \( S/F/T \) holds in general.

E.g. Show that \( 3^n - 1 \) is an even number for all \( n \geq 1 \).

**Base step:** \( n=1: \ 3^{1} - 1 = 2 \cdot 1 \cdot 1 = 2 \). \( \checkmark \)

**Inductive step:** Suppose \( 3^n - 1 \) is even for some \( n > 1 \).

To show that \( (TST) \ 3^{n+1} - 1 \) is even.

\[
3^{n+1} = (3^3)^n - 1 = \quad 3^n - 1 = 2k, \quad k \geq 1 \\
= (3 \cdot (2k+1) - 1) \quad \Rightarrow \quad 3^n = 2k + 1 \\
= 2 \cdot (3k) + 3 - 1 = 2 \cdot (3k) + 2 \\
= 2 \cdot (3k+1), \text{ hence even.} \]
Well-Ordering Property: Every non-empty set of positive integers has a least element.

Theorem: A set of positive integers that contains 1 and the integer n+1, whenever it contains n, must be the set of all positive integers.

Proof: Let S = \{Set of positive integers \mid 1 \in S, and whenever n \in S, then n+1 \in S\}.

To show: S = Set of all positive integers.

Suppose not.

Let T = Set of positive integers not in S.

Suppose T ≠ ∅: By WOP, the set T has a least element, say n. Thus n is a positive integer, n \in T, so n \notin S. Consider (n-1).

Note that n ≠ 1 as 1 \in S; hence n > 1.

By the property of n, we see that 0 ≤ n-1 \in S.

But if n-1 \in S, then n = (n-1)+1 \in S.

⇒ (Contradiction) as n \notin T. Hence T has to be the empty set ⇒ S = Set of all positive integers.
Theorem: If $a$ and $r$ are real numbers with $r \neq 1$, then
\[ \sum_{j=0}^{n} a r^j = a + ar + ar^2 + \ldots + ar^n = a \frac{r^{n+1} - 1}{r-1}. \]

Proof. By induction on $n$.

- **Base case ($n = 0$):**
  \[ a \cdot r^0 = a \cdot 1 = a = a \frac{r^1 - 1}{r-1}. \]

- **Inductive step ($n + 1$):**
  \[ a + ar = \text{LHS} = a (r+1). \]
  \[ \text{RHS} = a \frac{r^2 - 1}{r-1} = a (\frac{r+1}{r-1} \cdot \frac{r+1}{r-1}) = a (r+1). \]

Suppose (*) holds for $n$. Hence
\[ \sum_{j=0}^{n} a r^j = a \frac{r^{n+1} - 1}{r-1}. \]

To check that (*) holds for $n + 1$.
\[ \sum_{j=0}^{n+1} a r^j = a \frac{r^{n+2} - 1}{r-1} \]

\[ \text{LHS} = \sum_{j=0}^{n+1} a r^j = a \frac{r^{n+2} - 1}{r-1} + ar^{n+1} \]
\[ = a \frac{r^{n+2} - 1}{r-1} + ar^{n+1} \]
\[ = a \frac{r^{n+2} - a + ar^{n+2} - ar^{n+2}}{r-1} \]
\[ = a \frac{r^{n+2} - a}{r-1} = \text{RHS}. \]
\[
\sum_{i=0}^{n} \frac{3^i}{3^{i+1}} = 1 + 3 + 3^2 + \cdots + 3^n
\]

\[
a = 1, \quad r = 3, \quad \text{hence} \quad \sum_{i=0}^{n} a r^i = 1, \quad \frac{3^{n+1}}{3-1} = \frac{3^{n+1}}{2} = \frac{3^n}{2}
\]

\[\text{Def: A function } f \text{ is defined recursively if the value } f(1) \text{ is specified, along with a rule for determining } f(n+1) \text{ from } f(n). \]

\[\text{Eq. Def} f(n) = n! = n(n-1)(n-2) \cdots (1). \quad (0! = 1). \]

\[f(n) = n!, \quad f(n+1) = (n+1)! = (n+1) \cdot n! \]

\[\Rightarrow f(n+1) = (n+1) \cdot f(n). \]

\[\text{Def: Let } m \text{ and } k \text{ be non-negative integers with } k \leq m. \text{ The binomial coefficient } \]

\[
\binom{m}{k} = \frac{m!}{k! \cdot (m-k)!}, \quad \text{Not} \binom{m}{k} = \binom{m}{m-k}.
\]
\[ \binom{m}{0} = 1; \quad \binom{m}{k} = \frac{m!}{k!(m-k)!} \]
\[ = \frac{1 \cdot 2 \cdot 3 \cdots m}{(1 \cdot 2 \cdots k)(1 \cdot 2 \cdot 3 \cdots m-k)} \]
\[ = \frac{(m-k+1)(m-k)\cdots (m-1)m}{k!} \]
\[ \therefore \binom{6}{2} = \frac{6!}{2! \cdot 4!} = \frac{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{(1 \cdot 2)(4 \cdot 3 \cdot 2 \cdot 1)} = \frac{6 \cdot 5}{2} = 15. \]

Note: \[ \binom{n}{0} = \binom{n}{n} = 1 \]

Theorem: Let \( n \) and \( k \) be positive integers with \( n \geq k \).
Then
\[ \binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}. \]

Proof: \( \text{LHS} = \binom{n}{k} + \binom{n}{k-1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \]
\[ = \frac{n!(n-k+1)k}{k!(n-k+1)!} + \frac{n!k}{k!(n-k+1)!} \]
\[ \binom{n}{k} = \frac{n!(n-k+1)}{k!(n-k+1)!} = \frac{n!(n-k+1+k)}{k!(n-k+1)!} \]

\[ \frac{n!(n+1)}{k!(n-k+1)!} = \frac{(n+1)!}{k!(n-k+1)!} = \binom{n+1}{k} = \text{RHS.} \]

**Pascal's Triangle:** Displays binomial coefficient \( \binom{n}{k} \).

\( \binom{n}{k} \) is the \( k+1 \)th entry in the \( n+1 \)th row.

\[
\begin{array}{cccccc}
1 & 1 & 1 & \binom{3}{1} & = 2 & \text{entry} \\
1 & 2 & 1 & \binom{3}{0} & = 1 & \text{row} \\
1 & 3 & 3 & 1 & = 3 \\
1 & 4 & 6 & 4 & 1
\end{array}
\]

**Binomial Expansion:**

\[(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n}y^n.
\]

\[
\sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j.
\]

\((x+y)^3 = x^3 + \binom{3}{1}x^2y + \binom{3}{2}xy^2 + y^3\]

Proven by induction on \( n \).
Divisibility: Let $a, b$ be integers. Say $a$ divides $b$, denoted $a \mid b$, if there exists an integer $c$ such that $b = ac$.

Say $a$ is a divisor (or factor) of $b$.

If $a$ does not divide $b$, write $a \nmid b$.

E.g., $3 \mid 33$, $5 \nmid 26$.

**Proof:** If $a \mid b$ and $b \mid c$, then $a \mid c$.

Let $a \mid b \Rightarrow b = ac$; $b \mid c \Rightarrow c = bf$.

$\Rightarrow c = (ac)f = a(ef) \Rightarrow a \mid c$.

**Proof:** If $a, b, m, n$ are integers and $c \mid a$ and $c \mid b$, then $c \mid ma + nb$.

Let $c \mid a \Rightarrow a = ec$; $c \mid b \Rightarrow b = fc$.

Hence $ma + nb = mec + nfc = c(me + nf)$.

$\Rightarrow c \mid ma + nb$.

**Division Algorithm/Theorem:** If $a$ and $b$ are integers such that $b > 0$, then there are unique integers $q$ and $r$ such that $a = bq + r$, with $0 \leq r < b$. \(q\) \rightarrow quotient, \(r\) \rightarrow remainder.
Def: Let \( x \) be a real number. The greatest integer in \( x \), denoted \( \lceil x \rceil \), is the largest integer less than or equal to \( x \).

\[ \lceil 2.5 \rceil = 2; \quad \lceil -4.5 \rceil = -4; \quad \lceil -0.5 \rceil = 0. \]

Note: If \( x \) is a real number, then \( x - 1 < \lceil x \rceil \leq x \).

Proof of Division Algorithm: Let \( q = \lceil \frac{a}{b} \rceil \), and
\[ r = a - b \lceil \frac{a}{b} \rceil. \]

Claim: \( a = bq + r \), and \( 0 \leq r < b \).

Note \( \frac{a}{b} - 1 < \lceil \frac{a}{b} \rceil \leq \frac{a}{b} \)

Multiply by \( b \):
\[ a - b < b \lceil \frac{a}{b} \rceil \leq a \]

Multiply by \(-1\), note reverse inequality:
\[ -a < -b \lceil \frac{a}{b} \rceil < b - a \]

Add \( a \) throughout. Get:
\[ 0 < -b \lceil \frac{a}{b} \rceil + a < b. \]
Uniqueness: Suppose \[ a = bq_1 + r_1, \quad 0 \leq r_1 < b \]
\[ a = bq_2 + r_2, \quad 0 \leq r_2 < b. \]

Uniqueness \iff \( q_1 = q_2, \quad r_1 = r_2. \)

Subtract: \( 0 = b(q_1-q_2) + (r_1-r_2). \)
\[ \Rightarrow b(q_1-q_2) = r_2-r_1, \]
\[ \Rightarrow b \mid (r_2-r_1). \] But \( r_1, r_2 < b, \)
hence \( b \mid (r_2-r_1) \Rightarrow r_2-r_1 = 0. \)

But \( r_2 = r_1 \Rightarrow q_1 = q_2 \Rightarrow \text{Uniqueness}. \)

\[ a = 1535, \quad b = 35 \]
\[ 1535 = (35 \times 43) + 20 \]
\[ q = 43, \quad r = 20. \]
\[ a = 1551, \quad b = 5 \]
\[ 1551 = 5 \times 31 \]
\[ q = 31, \quad r = 0. \]
Def: A real number \( x \) is **rational** if there are integers \( p, q \) with \( q \neq 0 \) such that \( x = \frac{p}{q} \).

A real number \( x \) which is not rational is called **irrational**.

\[ \frac{23}{44}, \frac{1}{3} \text{ rational, } \frac{1}{3} \text{ rational} \]

\( \sqrt{2}, \pi, \frac{22}{7}, e \) are irrational.

**Theorem:** \( \sqrt{2} \) is irrational.

**Pf:** Suppose \( \sqrt{2} \) is rational. Then \( \exists \) positive integers \( a, b \) such that \( \sqrt{2} = \frac{a}{b} \), \( b \neq 0 \). (*)

Set \( S = \{ k\sqrt{2} \mid k \text{ and } k\sqrt{2} \text{ are positive integers} \} \).

(4) \( \Rightarrow S \) is not the empty set.

By the W.O.P., \( S \) has a least (smallest) element, say \( b = t\sqrt{2} \), \( t \text{ positive integer} \).

Consider \( (8\sqrt{2} - b) = (t\sqrt{2})\sqrt{2} - t\sqrt{2} \)

\[ = b\sqrt{2} - t\sqrt{2} \]
\[ = (b-t)\sqrt{2} \]
But \( 8\sqrt{2} = (4\sqrt{2})\sqrt{2} = 2t \), hence

\( 8\sqrt{2} \) and \( 8 \) are both integers. Also,

\((8\sqrt{2} - 8) = (8-t)\sqrt{2} \) is again an integer,
which is positive since \( \sqrt{2} > 1 \). Let \( u = (8\sqrt{2} - 8) \),
then \( u \in S \). But \( u < 8 \) and \( u \in S \) gives a contradiction. \( \Rightarrow \)

Hence \( \sqrt{2} \) is irrational.

\( \mathbb{Z}^+ \): Positive integers, \( \mathbb{Q} \): Rational numbers
\( \mathbb{R} \): Real Numbers

Def: A number \( \alpha \) is algebraic if \( \alpha \) is the root of a polynomial with integer coefficients
i.e. \( \exists \) a polynomial \( f(x) \in \mathbb{Z}[x] \) such that \( f(\alpha) = 0 \)

\( \iff a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots + a_1 \alpha + a_0 = 0 \), \( a_i \in \mathbb{Z} \).

Ex: \( \alpha \in \mathbb{Q} \Rightarrow \alpha \) is algebraic.

\( \alpha = \frac{m}{n}, \ m, n \in \mathbb{Z}, \ n \neq 0. \) Then \( \alpha \) satisfies

\( f(x) = nx - m = 0; \ f(x) \in \mathbb{Z}[x]. \)

\( \sqrt{2} \) is algebraic since \( \sqrt{2} \) satisfies \( f(x) = x^2 - 2 \in \mathbb{Z}[x] \).

\( \pi, \ e \) are not algebraic.
Def: A number $x$ is transcendental if $x$ is not algebraic.

Eg. $\pi, e$.

Notation:
- $\lfloor x \rfloor$ — Greatest integer function (largest integer $\leq x$); also denoted $\lfloor x \rfloor$ (floor function).
- Ceiling function: $x$ a real number, $\lceil x \rceil$ is the smallest integer greater than or equal to $x$.
  Eg. $\lceil \frac{7}{2} \rceil = 4$, $\lceil -\frac{3}{2} \rceil = -1$.

- The fractional part of a real number $x$, denoted $\{ x \}$ is defined as $\{ x \} = x - \lfloor x \rfloor$.
  Eg. $\{ \frac{7}{3} \} = \frac{7}{3} - \lfloor \frac{7}{3} \rfloor = \frac{7}{3} - 2 = -\frac{1}{3}$.
  $\{ -\frac{9}{5} \} = -\frac{9}{5} - \lfloor -\frac{2}{5} \rfloor = -\frac{9}{5} - (-1) = -\frac{9}{5} + 1 = \frac{3}{5}$.

$[\ ]$ — integral part; $\lceil \rceil$ — “Ceiling”
$\lfloor \rfloor$ — floor; $\{ \}$ — fractional part
$\mid \mid$ — absolute value; $\mid -x \mid = x, x > 0$. 
Theorem (Pigeonhole Principle): If \((k+1)\) or more objects are placed in \(k\) boxes, \(k \geq 1\) (integer), then at least one box contains two or more objects.

\[\text{Theorem: (Dirichlet's approximation theorem)}\]
\[\text{If } \alpha \text{ is a real number and } n \text{ is a positive integer, then there exist integers } a, b \text{ such that } 1 \leq a \leq n, \text{ and } |a \alpha - b| < \frac{1}{n}.\]

**Proof:** Consider the set of \((n+1)\) numbers defined
\[\{0, \{\alpha\}, \{2\alpha\}, \ldots, \{n\alpha\}\}.\]
We have
\[0 \leq \{j\alpha\} < 1, \quad 0 \leq j \leq n.\]
These \((n+1)\) numbers lie in the \(n\)-disjoint intervals \([k\alpha/n, (k+1)\alpha/n)\), \(0 \leq k \leq n-1\),
\[\{x \in \mathbb{R} \mid k\alpha/n \leq x < (k+1)\alpha/n\}.

By the Pigeonhole Principle (PHP), one of these intervals must contain at least two numbers.
Each interval has length \( \frac{1}{n} \), hence distance between any two (distinct) numbers in any of these intervals < \( \frac{1}{n} \).

\[ \Rightarrow \exists \text{ integers } j, k \text{ s.t. } 0 \leq j < k \leq n \text{ and } |\{ka\} - \{jd\}| < \frac{1}{n}. \] Put \( a = k - j \), and

\[ b = [ka] - [jd]. \] Then

\[ |a \cdot d - b| = |ka - jd - ([ka] - [jd])| \]

\[ = |(ka - [ka]) - (jd - [jd])| \]

\[ = |\{ka\} - \{jd\}| \]

\[ < \frac{1}{n}. \]

E.g. \( d = \sqrt{3} \approx 1.732 \), \( 2d \approx 3.464 \), \( 3d \approx 5.196 \),

\( 4d \approx 6.928 \), \( 5d \approx 7.660 \); let \( n = 2 \), \( \frac{1}{n} = 0.5 \).

For \( a = 2 \), \( b = 3 \), we have \( |a \cdot d - b| = |3.464 - 3| \)

\[ = 0.464 < 0.5 \] (a = n = 2).