Def: A set is **countable** if it is finite or if it is infinite and there exists a 1-1 correspondence between the set \( \mathbb{Z}^+ \) of positive integers and the given set.

A set that is not countable is **uncountable**.

**Ex:** \( \mathbb{Z}^+ \) is countable

- \( \mathbb{Z} = \{0, 1, -1, 2, -2, \ldots \} \)

\[
\begin{align*}
f : \mathbb{Z}^+ & \leftrightarrow \mathbb{Z} \\
n = 1 & \mapsto 0 \\
n > 1, n & \mapsto a_{2n} \quad \{ a_{2n+1} \leftrightarrow -n \}
\end{align*}
\]

- \( a_i \in \mathbb{Z}; \quad a_i = 0, \quad a_{2n} = n, \quad a_{2n+1} = -n \)

- \( \mathbb{Q} \), the set of rational numbers is **countable**.

- \( \mathbb{R} \), the set of real numbers is **uncountable**.
Greatest Common Divisor: $a, b \in \mathbb{Z}$ not both zero.

The greatest common divisor (gcd) of $a$ and $b$, denoted $(a, b)$, is the largest integer that divides $a$ and $b$.

If $(a, b) = d$, then $d \mid a$ and $d \mid b$.

Further if $c \mid a$ and $c \mid b$, then $c \mid d$.

E.g. $(25, 70) = 5$; $(120, 300) = 60$.

$(74, 27) = 1$.

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

Some interesting sequences of numbers:

1) Triangular numbers: $\{ t_1, t_2, t_3, \ldots \}$

$t_k = \text{number of dots in the triangular array with } k \text{ rows, and } j \text{ dots in the } j^{th} \text{ row}$

$\{1, 3, 6, \ldots \}$

$t_k = \sum_{b=1}^{k} b = \frac{k(k+1)}{2}$

2) Fibonacci Sequence: $\{1, 1, 2, 3, 5, 8, 13, \ldots \}$
Observe, if \( n \) is a positive integer, then for any real number \( x \), \( \left\lfloor \frac{x}{n} \right\rfloor = \left[ \frac{x}{n} \right] \).

Suppose \( [x] = m \). By the division algorithm, \( \exists \) integer \( q, r \) such that \( m = nq + r \), \( 0 \leq r \leq n-1 \).

Also \( q = \left[ \frac{m}{n} \right] \), and \( [x] \leq x < [x] + 1 \).

Hence \( x = [x] + \varepsilon \), with \( 0 \leq \varepsilon < 1 \).

\[ \Rightarrow \left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{[x] + \varepsilon}{n} \right\rfloor = \left\lfloor \frac{m + \varepsilon}{n} \right\rfloor = \left\lfloor \frac{mn + \varepsilon}{n} \right\rfloor = \left\lfloor \frac{m + \varepsilon}{n} \right\rfloor \]

\[ = \left[ q + \frac{\varepsilon}{n} \right] \]. But \( 0 \leq \varepsilon < n-1 \), and \( 0 \leq \varepsilon < 1 \)

\[ \Rightarrow 0 \leq \varepsilon + \frac{\varepsilon}{n} < (n-1) + 1 \Rightarrow 0 \leq \varepsilon + \frac{\varepsilon}{n} < n \]

\[ \Rightarrow \left[ \frac{x}{n} \right] = \left[ q \right] = q = \left[ \frac{m}{n} \right]. \]

**Def:** A **prime (\( \Rightarrow \) prime number)** is an integer \( > 1 \) which is divisible by no positive integer other than 1 and itself.

\( \therefore \) : \( 2, 3, 5, 7, 11, 23, \ldots \)

An integer \( > 1 \) which is not prime is called a **composite**:

\( \therefore \) : \( 6 = 2 \times 3, \ 21 = 3 \times 7, \ 121 = 11 \times 11, \ 1001 = 7 \times 11 \times 13 \).
Lemma: Every integer \( \geq 1 \) has a prime divisor.

Proof: Let \( m \in \mathbb{Z}^+, m \geq 1 \), suppose \( m \) has no prime divisor.

Let \( S = \{ k \in \mathbb{Z}^+ \mid k \text{ has no prime divisor} \} \).

Note \( S \neq \emptyset \) by our assumption, and \( m \in S \).

By the WOP, the set \( S \) has a least integer, say \( n \). As \( n \in S \), conclude that \( n \) has no prime divisors. In particular, \( n \) is not prime.

Hence \( n \) is composite \( \Rightarrow n = a \cdot b \), \( 1 \leq a < n \)

\( \Rightarrow a \mid n \).

Now \( a < n \Rightarrow a \notin S \Rightarrow \exists \) a prime \( p \) such that \( p \mid a \).

But \( p \mid a \) and \( a \mid n \), hence \( p \mid n \).

(contradiction).

Hence the lemma is proved.

Theorem (Euclid): There are infinitely many primes.

Proof: Suppose there are only finitely many primes, say \( p_1, p_2, \ldots, p_n \), \( n \in \mathbb{Z}^+ \). Let \( Q_n = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 \).

By lemma, \( \exists \) a prime \( q \) such that \( q \mid Q_n \). Say \( q = p_k \), \( 1 \leq k \leq n \). Then \( q \mid Q_n \), and \( q \mid p_1 \cdot p_2 \cdot \ldots \cdot p_n \).

\( \Rightarrow q \mid Q_n - (p_1 \cdot p_n) \Rightarrow q \mid 1 \), \( \Rightarrow \)
Theorem: There are infinitely many primes.

**Proof:** Suppose that there are only finitely many primes \( p_1, p_2, \ldots, p_n \), where \( n \in \mathbb{Z} \). Let

\[ Q_n = p_1 p_2 \cdots p_n + 1 \]

By the above lemma, there is a prime \( q \) s.t. \( q \mid Q_n \).

Now \( q = p_j \) for some \( 1 \leq j \leq n \), say \( q \mid p_j \).

\[ \Rightarrow 1 \mid Q_n \quad \text{and} \quad q \mid p_1 \cdots p_n \Rightarrow q \mid (Q_n - (p_1 \cdots p_n)) \]

\[ \Rightarrow q \mid 1 \Rightarrow q = 1 \Rightarrow \]

**Note:** The proof only tells us about the existence of infinitely many primes, but not how to find the next prime.

Theorem: If \( n \) is a composite integer, then \( n \) has a prime factor not less than or equal to \( \sqrt{n} \).

**Proof:** As \( n \) is composite, \( n = a \cdot b \), \( a, b \) integers \( 1 < a \leq b < n \). We must then have \( a \leq \sqrt{n} \), \( b \leq \sqrt{n} \), since otherwise \( b \geq a > \sqrt{n} \Rightarrow ab > \sqrt{n} \cdot \sqrt{n} \)

\[ \Rightarrow ab > n. \quad \Rightarrow \]

Can use this theorem to find all primes \( \leq n \), for \( n \in \mathbb{Z}^+ \). The method is called the sieve of Eratosthenes.

If \( n = 100 \), \( \sqrt{n} = 10 \).

Primes \( \leq 10 \) : 2, 3, 5, 7.

Hence every composite number \( < 100 \), has a prime divisor \( < 10 \).
Hence to check whether an integer \( k \leq 100 \), is prime, we must check for divisibility by \( 2, 3, 5, 7 \). Cross them out. Then check for divisibility by 3, next by 5, repeat.

\[ \text{eg.: primes } \leq 100 \setminus \{ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97 \}. \]

- Inefficient method to decide whether a given integer is prime or not.

**Def.** The function \( \pi(x) \), where \( x \) is a positive real number, denotes the number of primes \( \leq x \).

\[ \text{eg.: } \pi(10) = 4; \quad \pi(100) = 25. \]

- Arithmetic progression consisting of primes.

**Theorem:** (Dirichlet's Theorem on Primes in Arithmetic Progressions): Suppose that \( a \) and \( b \) are relatively prime, positive integers. Then the arithmetic progression \( a_n + b; \ n = 1, 2, 3, \ldots \) contains infinitely many primes.

- Largest known primes: primality proofs, Twin primes, primes can be tested in polynomial time.
Determination of Primes: How are primes distributed?

Gauss (1777–1855):

\[ \frac{x}{\log x}, \quad \text{Li}(x) = \int_2^x \frac{dt}{\log t} \]

Li(x): Area of the curve \( y = \frac{1}{\log t} \) above the \( t \)-axis from \( t = 2 \) to \( t = x \).

Gauss: \( \Pi(n) \) = No. of primes \( \leq n \) grows at the same rate as the function in \( \ast \).

Made precise in mid 19th Century.

Prime Number Theorem (J. Hadamard, 1896, Vallee Poussin)

Riemann zeta function (fn. cf. \( a \) variable)

\[ \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod (1 - \frac{1}{p^s})^{-1} \]

Theorem: The ratio \( \frac{\Pi(x)}{\left(\frac{x}{\ln x}\right)} \) approaches 1 as \( x \to \infty \), i.e., \( \lim_{x \to \infty} \frac{\Pi(x)}{\left(\frac{x}{\ln x}\right)} = 1 \).