Theorem: \( \mathbb{R} \) is uncountable

Proof (contradiction)

Assume \( \mathbb{R} \) is countable. We derive a contradiction. If \( \mathbb{R} \) is countable, then so is the subset

\[
S = (0, 1] = \{ x \in \mathbb{R} | 0 < x \leq 1 \}
\]

Since \( S \) is countable, its elements form the range of a sequence.
\[ S = \left\{ r_1, r_2, r_3, r_4, \ldots \right\} \]

Now each element of \( S \) has a unique* decimal expansion:

\[ r_1 = .d_{11}d_{12}d_{13} \ldots \]
\[ r_2 = .d_{21}d_{22}d_{23} \ldots \]
\[ r_3 = .d_{31}d_{32}d_{33} \ldots \]

where each \( d_{ij} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \).

*If a number has 2 decimal expansions choose the one having a tail consisting of all 9s, i.e. choose \( .4999\ldots \) instead of \( .5000\ldots \).
The above list contains all elements of \( S \). Define \( x \in S \) by the rule

\[
x = \cdots c_1 c_2 c_3 \cdots
\]

where

\[
c_i = \begin{cases} 4 & \text{if } d_{i,i} \neq 4 \\ 5 & \text{if } d_{i,i} = 4 \end{cases}
\]

Observe \( c_i \neq d_{i,i} \) for all \( i = 1, 2, 3, \ldots \), therefore \( x \neq r_i \) for any \( i \), and hence \( x \not\in S \). But clearly \( 0 < x \leq 1 \) by its very construction.

\( \therefore x \in S \). This contradiction shows our assumption was false, so

\( \mathbb{R} \) is uncountable.
Remark.

Proof discovered by Georg Cantor. "Cantor diagonal argument".

So \(|\mathbb{R}| \neq |\mathbb{N}|\).

Thus, if \(A_1, A_2, A_3, \ldots\)

is a seq. of countable sets, then their union

\[ \bigcup_{i=1}^{\infty} A_i \]

is also countable.

Proof: Same as proof that \(|\mathbb{Z}^+ \times \mathbb{Z}^+| = |\mathbb{Z}^+|\).
Proof.

There are only countably many computable numbers!

why? There are only countably many computer programs to compute them, since each program is a finite seq. of symbols from a fixed alphabet.

So most real numbers are not computable!
Thus,

Let \( S \) be a set, no function \( f : S \rightarrow \mathcal{P}(S) \) can be surjective.

**Proof.** Let \( f : S \rightarrow \mathcal{P}(S) \).

Define \( A = \{ x \in S \mid x \notin f(x) \} \subseteq S \).

Then \( A \notin \text{Range}(f) \), why?
Suppose \( f(x) = A \).

If \( x \in A \) then \( x \in f(x) \) so \( x \notin A \).

If \( x \notin A \) then \( x \notin f(x) \) so \( x \in A \).

So no such \( x \) can exist.

\( \therefore A \notin \text{Range}(f) \)

\( \therefore f \) is not surjective.
4.1 Divisibility and Congruence

**Definition**
Let $a, b \in \mathbb{Z}$, $a \neq 0$. We say $a$ divides $b$ if $b = ak$ for some $k \in \mathbb{Z}$.

Notation: $a \mid b$

We also say: $a$ is a factor of $b$

$a$ is a divisor of $b$

$b$ is a multiple of $a$

$b$ is divisible by $a$

**Example**
$3 \mid 24$ since $24 = 8 \times 3$

$5 \nmid 21$ since $21 \neq 5k$ for any $k \in \mathbb{Z}$. 
\[1. \text{ If } a, b, c, d \in \mathbb{Z} . \]

\begin{enumerate}
\item \[a \mid b \land a \mid c \Rightarrow a \mid (b+c) . \]
\item \[a \mid b \Rightarrow \forall d : a \mid bd . \]
\item \[a \mid b \land b \mid c \Rightarrow a \mid e . \]
\end{enumerate}

Proof of (i):

\[
\begin{align*}
\text{if } a \mid b & \Rightarrow b = ak_1 \text{ for some } k_1 \in \mathbb{Z} . \\
\text{if } a \mid c & \Rightarrow c = ak_2 \text{ for some } k_2 \in \mathbb{Z} .
\end{align*}
\]

\[ b + c = ak_1 + ak_2 = a(k_1 + k_2) \]

\[ \therefore a \mid (b + c) \text{ since } k_1 + k_2 \in \mathbb{Z} . \]
Proof of (3): exercise

Proof of (2):

Let \( d \in \mathbb{Z} \) be arbitrary.

\[ a \mid b \implies b = ak \text{ for some } k \in \mathbb{Z} \]

\[ \therefore \quad bd = (ak)d = a(kd) \]

\[ \therefore \quad a \mid bd \text{ since } kd \in \mathbb{Z}. \]

Remark:

1. \( 1 \mid a \) for all \( a \in \mathbb{Z} \) \((a = a \cdot 1)\)
2. \( a \mid a \) for all \( a \in \mathbb{Z} \) \((a = 1 \cdot a)\)
3. \( a \mid 0 \) for all \( a \in \mathbb{Z} \) \((0 = 0 \cdot a)\)
**Corollary**

Let $a, b, c, m, n \in \mathbb{Z}$. Then

$$a \mid b \land a \mid c \implies a \mid (mb + nc)$$

**Proof**

$$a \mid b \implies a \mid mb$$

$$a \mid c \implies a \mid nc$$

by G1

$$a \mid (mb + nc)$$

by (25)

another proof:

$$a \mid b \implies b = ak_1 \implies mb = a(mk_1)$$

$$a \mid c \implies c = ak_2 \implies nc = a(nk_2)$$

$$\therefore mb + nc = a(mk_1 + nk_2)$$

$$\therefore a \mid (mb + nc)$$

since $mk_1 + nk_2 \in \mathbb{Z}$.
The (Division Algorithm)

Let \( a \in \mathbb{Z} \), \( d \in \mathbb{Z}^+ \). Then there exist unique \( q, r \in \mathbb{Z} \) such that:

\[ a = dq + r \quad \text{and} \quad 0 \leq r < d \]

We call: a dividend, \( d \) division, \( q \) quotient, \( r \) remainder.

Proof (existence only)

Let \( q = \left\lfloor \frac{a}{d} \right\rfloor \), and \( r = a - dq \).

Then \( a = dq + r \). Also
Then necessarily \( \theta = \frac{1}{2} \) and \( \alpha = \frac{1}{4} \).

\[
\alpha = d^2 + \gamma \quad \text{and} \quad \theta \leq \gamma < d
\]

**Exercise:** Prove uniqueness.

\[
f \leq \frac{9}{d} + \frac{1}{9} \quad \text{for} \quad \gamma > d
\]
Example:

123 = 12 \cdot 10 + 3, \quad 0 \leq 3 < 12

91 = 11 \cdot 8 + 3, \quad 0 \leq 3 < 11

-35 = 8(-5) + 5, \quad 0 \leq 5 < 8