2017

# Proof techniques.

- direct proof.
- Vacuous proof.
- trivial proof
- proof by contrapositive.
- proof by contradiction
- proof by cases.
- constructive existence proof.
- non-constructive existence proof.
- Uniqueness proof.
- mathematical induction
- structural induction
- well-ordering principal.
- Center diagonalization argument.
- combinatorial proof.

eg:- proof it by giving a solution.

CRT (Chinese Remainder Theorem). { Constructive Existence proof }.

① $\begin{cases} x = a_1 \bmod n_1 \\ x = a_2 \bmod n_2 \\ \vdots \\ x = a_k \bmod n_k \end{cases}$ $n_1, n_2, \cdots, n_k \rightarrow$ pairwise relatively prime (Coprime)

$N = n_1 \cdot n_2 \cdot n_3 \cdots \cdot n_k$.

solution of ① mod N

$N_i = \frac{N}{n_i}$, $M_i = N_i^{-1} \bmod n_i$

$\hookrightarrow M_i N_i = 1 \bmod n_i$

Scanned by CamScanner

Claim

$$x = \sum_{i=1}^{k} a_i M_i N_i \mod N$$ solution of (1).

Eg:- $Z_{13} = \{0, 1, 2, \ldots, 12\}$.

$2^{-1} \mod 13$.

$a \in Z_{13}$ such that $a(2) = 1 \mod 13$.

$a^{-1} = 2$. $\boxed{a = 7}$

$a = 2^{-1}$

$x = a_1 M_1 N_1 + a_2 M_2 N_2 + \cdots + a_k M_k N_k \mod n_i$

$= 0 + 0 \cdots + \underbrace{a_i M_i N_i}_{= a_i \bmod n_i} + 0 + 0 \cdots 0$

Similarly Non-constructive proof → giving the proof without constructing a solution.

Uniqueness proof:-

Division Algorithm ⇓ or FTA (fundamental theorem of arithmatic)

$a = bq + r$, $0 \le r < b$ ; $q, r$ unique

$(a > b)$

FTA ⇒ $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_n^{\alpha_n}$

$p_1, p_2, \ldots, p_n$ are distinct primes

unique → $p_1 < p_2 < p_3 < \cdots < p_n$.

{any integer N can be expressed in the above stated way}.

Scanned by CamScanner

## Centre Diagonalization Argument.

↳ deals with set theory.

* compare between two set of infinite size (cardanality).

## Russel's paradox.

Let S be the set of all sets that do not include themselves.

Does S contain itself?

$S = \{x \mid x \notin x\}$. , domain of discourse be the set of all sets.

Case ① Suppose. → S is not a member of itself

or

Case ② Suppose. → S is a member of itself.

## Illustration of Russel's paradox.

→ Suppose every library in the US is preparing a database of all its collections

→ From across the country, all the databases are submitted to the Library of Congress.

National Librarian makes two databases.

| Database 1 | Database 2 |
|---|---|
| that include themselves | that do not include themselves. |

where to put database 2 that do not include themselves.

— if listed., it should be listed in Database 1 {giving a contradiction}.

— if not listed → not a true database.

* no solution exists to this type of problem $S = \{x \mid x \notin x\}$.

* wants to make a database that do not include themselves.

NEXT CLASS → Cardanality of sets.

Scanned by CamScanner

27.2.2017

# Cardinality of sets. (infinite) {Dedekind, 1888}.

→ If A & B are infinite sets, and $A \subset B$, then $|A| = |B|$. (TRUE).

Eg:- $N = \{1, 2, 3, 4, \ldots\}$. (unbounded).

$S = \{3, 6, 9, 12, \ldots\}$, multiple of 3.

$S \subset N$. (we can always make one-to-one correspondance matching).

$f: N \to S$. ← one-to-one correspondance (bijection).

{A part of it is the whole}.

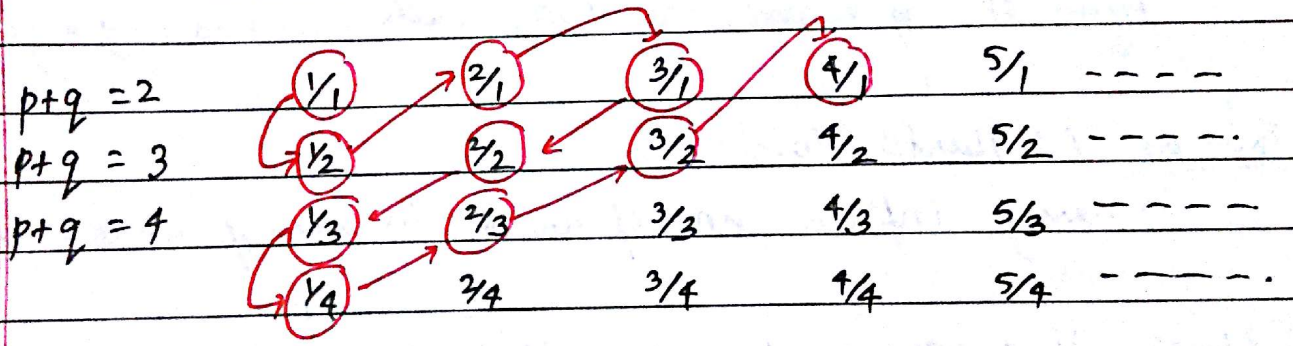
S → infinite sets.

P(S) ← power set.

Example.

all rational nos. (p/q)

countables or

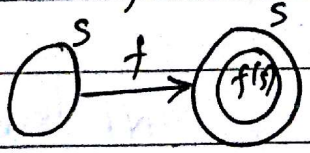



Finite set. → S finite with cardanility n if ∃ a bijection, $\{0, 1, 2, \ldots, n-1\}$ to

Infinite set. → A set S is infinite if. ∃ an injection $f: S \to S$ such that f(s) is a proper su

countable

uncountable




elements of S can be listed a sequence $\{a_n\}$.

eg:- N → the set s of all numbers (natural). is infinite.

injection. : $f: N \to N$ defined by. $f(x) = 3x$.

$f(N) = \{3, 6, 9, \ldots\} \subset N = \{1, 2, \ldots, N\}$

⇒ N is an infinite set.

Scanned by CamScanner

$N \rightarrow$ infinitely countable.
Rational nos. $\rightarrow$ infinitely countable.

classmate
Date
Page

**Countable set** → that has the same cardanality as the set of natural nos.

$|N| = \aleph_0$ (aleph null).

**Uncountable set** → that is not countable.

**Example.** (Coffee Beans). {Finite # of coffee beans}.
- dark & light roasted coffee beans.
- without counting them explicitely, to decide whether there is an equal no. of dark roasted and light roasted coffee beans.

(try to find a match between dark & light roasted)

~~now, consider if there are.~~
~~INFINITE.~~

**Example** (Finite Hotel)
Finite # of rooms, say 100, each occupied by a guest.

**Example** (Hilbert's Hotel)
↳ having infinite no. of rooms. in each of which a guest is staying.

→ Suppose if a new guest comes, if finite Hotel, then he cannot fit in the hotel.

→ In case of infite Hotel, ask guest in room n to shift to room n+1.

$|N| = \aleph_0$ ① ③ ⑤
$\aleph_0 + 1 = \aleph_0$ ② ④ ⑥ ...
$\aleph_0 + 2 = \aleph_0$.
⋮
$\aleph_0 + \aleph_0 = \aleph_0$.

a transfinite no.

$|P(N)| = \aleph_1$ (aleph Null)
$|P(P(N))| = \aleph_2$

$|N| < |P(N)| < |P(P(N))| < - - -$
$\aleph_0 \quad \aleph_1 \quad \aleph_2$

(N) P(N) P(P(N))

Scanned by CamScanner

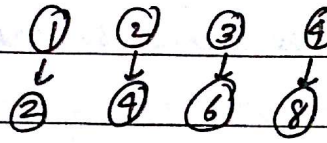
S is any infinite set then $|S| < |P(S)|$.

$|A| \leq |B|$, if $\exists$ a injection from A to B. ; A & B are infinite sets.

$|A| = |B|$ ; A & B are equipotent, if $\exists$ a bijection from A to B.

~~Assume, suppose~~ if $|A| < |B|$ → no bijection from A to B but an injection from A to B.

now, suppose, if infinite no. of guests come. then we may ask guest in $n^{th}$ room to shift to $2n^{th}$ room. All the even rooms are then vacanted, then fit the new guests i in the $(2i-1)$ rooms.




$\aleph_0 \times 1 = \aleph_0$.

$\aleph_0 \times 2 = \aleph_0$.

$\aleph_0 \times 3 = \aleph_0$.

⋮

$\aleph_0 \times \aleph_0 = \aleph_0$

NEXT CLASS → set of Real nos. (R) → [0, 1]. (subset) } uncountable. { proof by contradiction }

Scanned by CamScanner

Uncountable Set → not countable → $|S| \neq |\mathbb{N}| = \aleph_0$.
→ no listing of elements of S in a row? (an)
→ no bijection from S to N.
→ not enumerable.

Definition → (Enumeration)
Let S be a set.
An enumeration of S is a surjection and from the initial line segment of N to S.
- with repetition
- without repetition.

- additionally if f is also injective, then f is an enumeration without repetition.
- f not injective, then f is an enumeration with repetition.

Example → S = the set of natural nos. of the form $3n$, $n \in \mathbb{N}$
- $<0, 3, 6, 9, 12, \dots>$ → $f(n) = 3n$. $(k=0)$
- $<6, 3, 0, 15, 12, 9, \dots>$

$$f(n) = \begin{cases} 3n+6, & \text{if } n = 3k \text{ for some integer } k. \\ 3n, & \text{if } n = 3k+1 \text{ for some } k \in \mathbb{N} \\ 3n-6, & \text{if } n = 3k+2 \text{ for some } k \in \mathbb{N} \end{cases}$$

Examples

1. Set of all odd integers.
2. Set of all even integers.
3. Set of all ~~natural~~ nos. (rational nos.).
4. Set of all integers. → $0, +1, -1, +2, -2, \dots$

$$f(n) = \begin{cases} n/2, & \text{if } n \text{ is even} \\ \frac{n-1}{2}, & \text{if } n \text{ is odd} \end{cases}$$

1 2 3 4 5
↕ ↕ ↕ ↕ ↕
$0, +1, -1, +2, -2, \dots$

one-to-one mapping.

Scanned by CamScanner

## Example (uncountable set)

**Theorem** → R, the set of all real nos. is uncountable

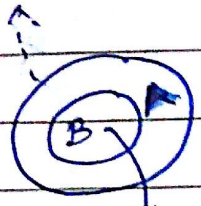
**Proof** → (by contradiction).

Suppose R is countable

given A is countable.

**Claim 1** → Any subset of a countable set is also countable.

**Claim 2** → Any superset of an uncountable set is uncountable.




given B is uncountable.

Prove that superset A of B is uncountable. (Claim 2)

If not i.e. if A is countable.

⇓

there exists a listing $\{a_n\}$ of elements of A.

↓

take the subsequence $\{b_n\}$ of elements of $B \subseteq A$

B is countable {contradiction}. (→←)

Similarly, proof Claim 1.

**Proof of the theorem.**

Suppose R is countable.

$[0,1] \subset R$ by Claim 1 is countable.

* If it is countable then there is a listing.

$r_1, r_2, \ldots$, a listing of the elements of $[0,1]$ in some order.

LIST (1)

$r_1 = 0.d_{11}\, d_{12}\, d_{13}\, d_{14} \ldots$

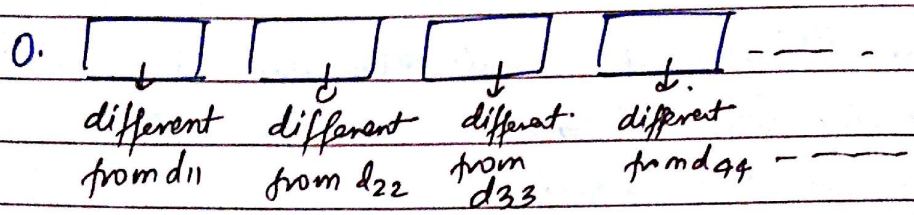
$r_2 = 0.d_{21}\, d_{22}\, d_{23}\, d_{24} \ldots$

$r_3 = 0.d_{31}\, d_{32}\, d_{33}\, d_{34} \ldots$

$r_4 = 0.d_{41}\, d_{42}\, d_{43}\, d_{44} \ldots$

Scanned by CamScanner

construct a real no. as follows.




This is a real no. but it cannot be in the list ①.

∴ contradicting (→ ←) that [0,1] is countable.

so [0,1] is uncountable.

∴ By Claim 2, R is uncountable.

[0,1] → sometimes called continuumm

other consequences.

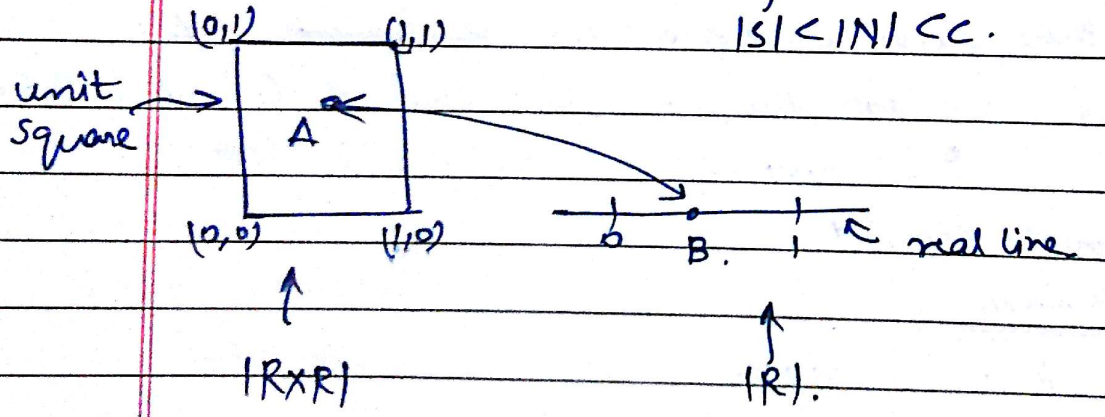
$|N| = \aleph_0$

$|[0,1]| = c$.

S → finite set.

$|S| < |N| < c$.

$|R \times R| = |R|$.




every point on a unit square can be mapped to a point on the real line [0,1].

Scanned by CamScanner

Example

$\Sigma = \{a, b\}$.

$\Sigma^*$ → set of all strings over $\Sigma$

$\{\varepsilon, a, b, aa, ab, ba, bb, \ldots\}$.

$\varepsilon$ (epsilon) → string of length zero.

countable set.

enumeration $\tau$ of $\Sigma^*$ $\quad \tau(31) = ?$

| power set of $\Sigma^*$ $P(\Sigma^*)$ is uncountable. |
|---|

Theorem

$\Sigma$ → a finite alphabet.

$\Sigma^*$ → the set of all strings over $\Sigma$

The $P(\Sigma^*)$, the power set of $\Sigma^*$, is uncountable.

proof :- (using Cantor's diagonalization argument).

↳ (by contradiction).

Suppose $P(\Sigma^*)$ is countable

$\langle A_0, A_1, A_2, \ldots \rangle$ be an enumeration of the element of $P(\Sigma^*)$.

As $\Sigma^*$ is countable, let $\langle x_0, x_1, x_2, \ldots \rangle$ be an enumeration of string in $\Sigma^*$

construct a binary matrix M as follows.

| | $x_0$ | $x_1$ | $x_2$ | $x_3$ ... |
|---|---|---|---|---|
| $A_0$ | $a_{00}$ | $a_{01}$ | $a_{02}$ | $a_{03}$ ... |
| $A_1$ | $a_{10}$ | $a_{11}$ | $a_{12}$ | $a_{13}$ ... |
| $A_2$ | $a_{20}$ | $a_{21}$ | $a_{22}$ | $a_{23}$ ... |
| ⋮ | | | | |

$$B = (a_{ij}) = \begin{cases} 1, & \text{if } x_j \in A_i \\ 0, & \text{otherwise} \end{cases}$$

Scanned by CamScanner

Now, construct a set A as follows:-

$x_i \in A$ if $q_{ii} = 0$.

i.e. if $x_i \notin A_i$

$A = \{x_i \in \Sigma^* \mid x_i \notin A_i \;, i \in N\} \subseteq P(\Sigma^*)$

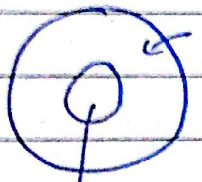
$\Downarrow$ $x_i \in A \Rightarrow x_i \notin A_i$

$\rightarrow$ A cannot be any of $A_i$ in the list M.

$P(\Sigma^*)$, $[0,1]$ } both uncountable.

Q. Can we compare the cardinality of two uncountable sets.?

→ all countable sets having the same cardinality No.




sequence $(i \to q_i) \to \{q_n\}$. identify a subset that is infinitely countable.

Theorem →. Consider any infinite set S.

Then S has a countably infinite subset.

$a_0 \in S$.

$q_1 \in S - \{a_0\}$.

$a_2 \in S - \{q_0, q_1\}$.

$\vdots$

$a_{n+1} \in \underbrace{S - \{q_0, q_1, \cdots, a_n\}}_{\text{infinite.}}$. ← CLAIM

if not, i.e. $S - \{q_0, q_1, \cdots, q_n\}$ is finite.

then $\{S - \{q_0, q_1, \cdots, q_n\}\} \cup \{a_0, q_1, \cdots, q_n\}$ finite.

$\therefore S \to$ finite $(\to \leftarrow)$.

Scanned by CamScanner

* If a bijection is involved then we can compare.

**Definition** → Let $S, T$ be two sets.
Then $S$ & $T$ are equipotent or have the same cardinality, denoted by $|S| = |T|$, if there is a bijection from $S$ to $T$.

**Theorem** → equipotence is an equivalence relation.

**Definition** →
- $|S| \leq |T|$ if there is an injection from $S$ to $T$.
- $|S| < |T|$ if there is an injection from $S$ to $T$ but no bijection
- either $|S| < |T|$ or $|S| = |T|$ or $|S| > |T|$.
- $|S| \leq |T|$ & $|T| \leq |S| \Rightarrow |S| = |T|$.

**Theorem** → $S$ → finite set. $c = |[0,1]|$ ← cardinality of $[0,1]$
$|S| \leq \aleph_0 < c$.

**proof** :- $|S| = n$.
$= |Z_n|$

$Z_n = \{0, 1, 2, 3, \ldots, n-1\}$.
$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \quad \downarrow$
$1 \quad 2 \quad 3 \quad 4 \quad \ldots \quad n$.

$f(x) = x + 1$.
$f : Z_n \to N$.

$\boxed{f(x) = \frac{1}{n+2}}$

$f : N \to [0,1]$.

$1 \quad 2 \quad 3 \quad 4 \quad \ldots$
$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow$
$\frac{1}{2} \quad \frac{1}{3} \quad \frac{1}{4} \quad \frac{1}{5} \quad \ldots$

also as $[0,1]$ is uncountable there is no bijection from $[0,1]$ to $N$
$|N| < |[0,1]|$ i.e. $\boxed{\aleph_0 < c}$

Scanned by CamScanner

**Theorem** :→ If S is an infinite set, then $\aleph_0 \leq |S|$.

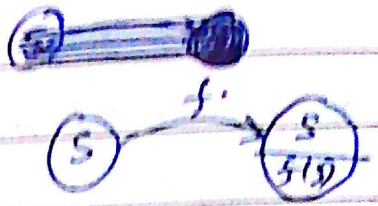
**proof** :→ eg:- $\mathbb{N}$

$3\mathbb{N} \subseteq \mathbb{N}$

$f(x) = 3x$.

$f: \mathbb{N} \to \mathbb{N}$

$f(\mathbb{N}) = 3\mathbb{N} \subset \mathbb{N}$




$f: S \to S$.

$f(S) \subset S$.

**proof**

$S' = \{a_n\}$. $S \to$ infinite.

→ Infinitely countable subset of S.

consider the mapping.

$f: S' \to S$.

defined by $f(x) = x$.

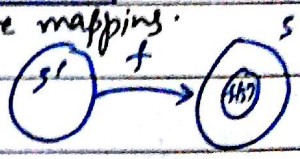
injective mapping.

$f: S' \to \mathbb{N}$

$|\mathbb{N}| = |S'| = \aleph_0$.

$\aleph_0 = |S'| = |f(S')|$

$\leq |S|$




**NEXT CLASS** → Try to prove the following.

$S \to$ infinite

$P(S) \to$ power set.

$|S| < |P(S)|$.

Scanned by CamScanner

3.2017

## Well-Ordering and Mathematical Induction.

$N \rightarrow$ set of all natural nos.

$S \subseteq N$, $S \neq \phi$ ↓ has a least element } Well-ordering principle.

**Example:-**

Prove that $n < 2^n$, $n \geq 1$.

using well-ordering principle.

**solution:-**

$S$ = set of natural nos. for which the inequality does not equality. $= \{ n \in N \mid n \geq 2^n \}$.

Claim $\rightarrow$ $S = \phi$

proof of the claim.

$S \subseteq N$

if $S = \phi$, then by well-ordering principle, $S$ has a smallest element, say $m$.

so for this $m$, $m \geq 2^m$. holds.

$\Rightarrow \boxed{\frac{m}{2} \geq 2^{m-1}}$ — (1)

Also, $1 \not\geq 2^1$

$1 \notin S$

$m \neq 1$, $\boxed{m \geq 2}$

$m + m \geq 2 + m$

$2m - 2 \geq m \Rightarrow \boxed{m - 1 \geq \frac{m}{2}}$ — (2)

Using (1) & (2)

$2^{m-1} \leq \frac{m}{2} \leq m - 1$.

→ we are getting $(m-1)$ which is smaller than $m$. (Try to find an element smaller than $m$).

Scanned by CamScanner

This contradicts to the ~~so~~ choice of $m$ as $m$ is the smallest element of $S$ & $m-1 < m$.

## Mathematical Induction

**First principle of finite induction.**

Given $S \subseteq N$, if (i) $1 \in S$ (base case)

(ii) $n \in S \Rightarrow n+1 \in S$. (inductive case)

then $S = N$.

**proof this by using (well-ordering principle).**

$S \subseteq N$ with conditions ① & ②, let $T = N/S$ $(N-S)$

claim :- $T = \phi$

↳ if $T \neq \phi$, get a contradiction.

well-ordering principle, 'a' is the smallest element of T.

$a \in T \Rightarrow (a-1) < a \rightarrow (a-1 \geq 0)$ ??

$\downarrow$

$\notin T$

$a-1 \in S$.

claim that $a \neq 1$.

$a-1 \in S$

↳ implies by (ii) $(a \in S)$ is a contradiction.

claim

$0 < a-1 < a$.

Scanned by CamScanner

- **Second principle of finite induction.**
  ↳ stronger version.

Given $S \subseteq N$, if (i) $1 \in S$ (base case)

(ii) $1, 2, 3, \cdots, n \in S \Rightarrow n+1 \in S$. (inductive case).

then $S = N$

Proof → (Try the same for second principle also). ← EXERCISE.

---

$T = N/S \ (N-S)$

claim, $T = \emptyset$

↳ proof of the claim. (by contradiction).

let $T \neq \emptyset$

Then $T \subseteq N$; non-empty

By well-ordering principle, T has a least element, say a

Formal proof of 1st principle.

$1 \in S$ ⇓ $a > 1$

$1 \in N$ ⇓ smallest element of N.

$0 < a-1 < a$ ↓ $\in T$.

$1 \in S$, $a-1 \in S$ ⇒ $a \in S$ (contradicti

as $a \in T$

as $a-1 < a$, $a-1 \notin T$

⇒ $a-1 \in S$. ∴ $T = \emptyset$

⇒ $S = T$.

Example (Mathematical Induction)

$P(n)$: $1+3+5+\cdots+(2n-1) = n^2$

Proof :- Base step. ; $1 = 1^2 \Rightarrow P(1)$ true.

Inductive step ; $P(1), P(2), \cdots, P(K)$ true.

claim: $P(K+1) \rightarrow$ true.

Scanned by CamScanner

$1 + 3 + 5 + \cdots + (2k-1) + (2k+1) = k^2 + (2k+1)$

$= (k+1)^2$.

(by induction hypothesis. $= k^2$)

$\Rightarrow P(k+1)$ is True.

→ The main disadvantage of this is that we have to GUESS.

$1 = 1^2$

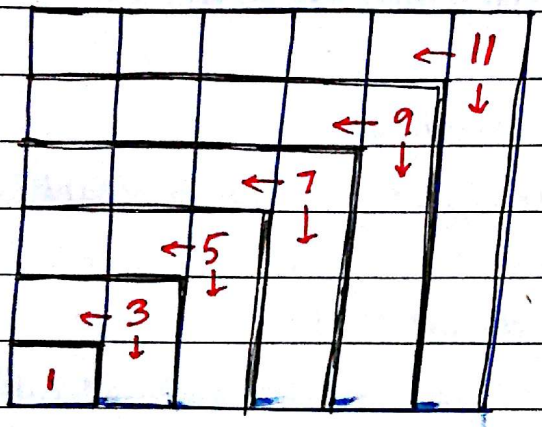
$1+3 = 2^2$

$1+3+5 = 3^2$

⋮

$n = 6$

consider a 6×6 square.




Area $= 6 \times 6 = 36$ unit$^2$

$= (1+3+5+\cdots+11) = 36$.

Example. (educated guess may not work)

$p(n)$ → # of partitions of $n$.

| | | partitions |
|---|---|---|
| $n=1$ | $p(1)=1$ ~~$p(n)=1$~~ | $p(1)=1$ $\quad 1 \to 1$. |
| $n=2$ | $p(2)=2$ | $2 \to 2$ or $(1+1)$ |
| $n=3$ | $p(3)=3$ | $3 \to 3$ or $(1+2)$ or $(1+1+1)$ $(1+2)$ and $(2+1)$ considered SAME |
| $n=4$ | $p(4)=5$ | $5 \to (1+1+1+1+1)$ or $(2+3)$ or $(1+1+3)$ or $(1+1+1+2)$ or $(1+4)$ |

↑ all were prime

but $p(7)=15$ → not a prime {guess did not work}.

Read About

Conjecture → $P(n)$ is prime

↓ FALSE

• $p(n)$ → complicated function

G.H. Hardy, Ramanujan London, Cambridge University Press 1990 } Ch. 6,8

Scanned by CamScanner

## Divison Algorithm:

$a, b$ two integers. , $b \geq 1$

then, $a = bq + r$ ; $0 \leq r < b$.

$q, r \rightarrow$ an integer (UNIQUE).

→ we have to ensure the bound on $r$ and the uniqueness.

proof: → (using Well-Ordering Principle)

consider the set $S = \{ a - bx \mid x \in Z, a - bx \geq 0 \}$

claim → $S \neq \emptyset$

$b \geq 1 \Rightarrow |a|b \geq |a|$.

$a + |a| \cdot b \geq |a| + a \geq 0$

$x = -|a|$.

$\therefore a + |a| \cdot b \in S$.

~~SHHH~~ By well-Ordering principle;

$S$ has a least element, say $r$.

$r = 0$ or $r > 0$.

↑ separate case.

(since well ordering principle defined for greater than zero)

$\therefore \exists\ q \in Z$ such that $r = a - bq$.

next claim → $r < b$.

if not, let $r \geq b$.

Then, $a - (q+1)b = (a - bq) - b = r - b \geq 0$.

and $a - (q+1)b$ is smaller than $a - bq$. implies

$a - (q+1)b \in S$

↳ which is a contradiction.

Scanned by CamScanner

17 **Divison Algorithm:**

$(b \neq 0)$

$a, b$ integers, $b \geq 1$.

$\exists$ unique integers $q$ (quotient) and $r$ (remainder) such that $\boxed{a = b \cdot q + r, \quad 0 \leq r < b}$

**Uniqueness.**

if not, let $\begin{cases} a = b \cdot q + r_1, & 0 \leq r_1 < b \\ a = b \cdot q' + r_2, & 0 \leq r_2 < b \end{cases}$

$0 \leq r_2 \leq b$

$-b \leq -r_1 \leq 0$

$-b < r_2 - r_1 < b.$

$|r_2 - r_1| < |b|$

$\Rightarrow b \cdot (q - q') = r_2 - r_1.$

$|b| \cdot |q - q'| = |r_2 - r_1| < |b|.$

$|q - q'| < 1 \Rightarrow q = q'$ (since $q$ & $q'$ are integers)

**Theorem.**

Given integers $a, b, b \neq 0$, $\exists$ unique integers $q, r$ such that $a = b \cdot q + r, \quad 0 \leq r < b.$

**proof:-** **case 1** → $b > 0$, i.e. $b \geq 1$. (already proofed)

**case 2** → $b < 0 \Rightarrow |b| > 0$

$\therefore$ By previous case, $a = |b| \cdot q' + r, \quad 0 \leq r < |b|$

$= -b \cdot q' + r, \quad (|b| = -b \text{ as } b < 0)$

$= b \cdot q + r, \quad q = q'$

**Bezout's Identity:**

Let $a, b$ be two integers, not both zero.

Let $d = \gcd(a, b)$

then $\exists$ integers $x$ and $y$ such that $d = ax + by$

(Extended Euclidean Algorithm).

Scanned by CamScanner

a, n be two integers.

$gcd(a,n) = 1 = ax + ny$, $x, y \in Z$.

$ax \equiv 1 \pmod n$. *. This method provides a way to find modular inverse.

congruence

$a^{-1} \equiv x \pmod n$

$a \equiv b \pmod n$
$n \mid (a-b)$.
then $a = nq + r$.
$b = nq' + r$.

} CONGRUENCE

Z (partition) (concept) form congruence

| | | | |
|---|---|---|---|
| 0 | 1 | . | . |
| - | . | . | r |
| | | | |

→ find $2^{-1} \bmod 5$.

then $2 \times x = 1 \pmod 5$

$\therefore x = 3 \quad \therefore 2^{-1} = x = 3$.

Extended Euclidean Algorithm → gives a procedure (algorithm) to find the inverse of any number.

$2^{-1} \bmod 5 = 3$. $2^{-1} \bmod 253 = ?$

Input → a, b.

find → (x, y, d)

$d = ax + by$

$a^{-1} \bmod n$ means. $\exists x \in \{1, 2, \dots, n-1\}$ such that $ax \equiv 1 \pmod n$.

↳ (x)

Scanned by CamScanner

## Proof (by Bezout's identity)

$$S = \{ax + by > 0 \mid x, y \in \mathbb{Z}\}.$$

Then $S \subseteq \mathbb{N}$

claim → $S \neq \emptyset$

$0 < |a| = ax + b.$

Take $x = \begin{cases} 1, & \text{if } a > 0 \\ -1, & \text{if } a < 0. \end{cases}$

$\Rightarrow |a| \in S.$

So, S is a non-empty subset of the set of natural nos. and therefore, by well-ordering principle, S must have a smallest element, say d.

$d$ = smallest element of $S$.

as $d \in S \Rightarrow d = ax + by$ for some integers x & y.

claim → $d \mid a$, $d \mid b$.

proof of the claim ↳ By division algorithm, $a = d \cdot q + r$, $0 \leq r < d$.

if $r \neq 0$, then $r = a - d \cdot q = a - (ax + by) \cdot q$

$= a(1 - xq) + b(-y)$

i.e. $r > 0$

$r \in S$, but $r < d$

contradiction (→)(←) to the choice of d.

so $\boxed{r = 0}$.

claim → $d = \gcd(a, b)$

↳ proof of the claim:

Let c be any other common divisor of a, b, i.e. $c \mid a, c \mid b$

$\Rightarrow c \mid ax + by \Rightarrow c \mid d \Rightarrow d$ is the gcd of a, b.

definition: ; $d = \gcd(a, b)$

i) $d \mid a$, $d \mid b$.

ii) any other common divisor, say, C, then $c \mid d$.

Scanned by CamScanner

# Fundamental Theorem of Arithmetic (FTA)

Every (+ve) integer, $a > 1$ can be uniquely expressed as the product of primes. In other words, there exists unique prime nos. $p_1 < p_2 < p_3 < \cdots < p_n$ and corresponding positive exponents $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{Z}_+$, such that

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \cdots \cdot p_n^{\alpha_n}.$$

That's why 1 is not considered as a prime because.

$15 = 1 \times 3 \times 5 = 1^2 \times 3 \times 5 = 1^3 \times 3 \times 5$, therefore, not a unique representation.

## Proof (by contradiction)

Suppose there were some (+ve) integers greater than 1 that were not expressible as a product of primes.

↳ $S$ be collection of these (+ve) integers.

Then $S$ is a non-empty subset of $\mathbb{N}$, therefore by well-ordering principle, $S$ has a smallest element, say $n$.

• '$n$' is not a prime.

$\Rightarrow n$ is composite

i.e., $n = a \cdot b$, $1 < a, b < n$.

↳ contradiction. ($\rightarrow\leftarrow$)

$a, b \notin S \Rightarrow a, b$ have their unique prime factorisation, which in turn gives a prime factorization of $n$.

$\Rightarrow n \in S$ ($\rightarrow\leftarrow$) as $n \notin S$.

Scanned by CamScanner

~~proof~~

Uniqueness:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_n^{\alpha_n} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_3^{\beta_3} \cdots q_r^{\beta_r}$$

$\alpha_i, \beta_i > 0$ (integers)

disjoint sets: $p_1 < p_2 < \cdots < p_n$ ; $q_1 < q_2 < \cdots < q_n$.

$p_i \mid p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_r^{\beta_r}$ | as $p_i, q_j$ are primes $p_i = q_j$

$\Rightarrow p_i \mid q$ ; for some $j$ ($\rightarrow\leftarrow$) contradiction.

Existence proof of FTA. (using weak induction).

$P(n) \rightarrow n$ can be written as product of primes.

Basis step $\rightarrow$ 2 can be written as product of 1 prime namely 2.

$\Rightarrow P(2)$ is True.

Inductive Step: Let $P(K)$ be true, i.e. K is written as a product of primes

claim $\rightarrow$ $P(K+1)$ is true.

consider integers $(K+1)$

- prime $\rightarrow$ $P(K+1)$ is true
- composite. $\rightarrow$ $K+1 = ab$ ; $2 \le a \le b < K+1$.

we need strong induction, we cannot go beyond

forward this with weak induction.

now, using strong induction.

$K+1 = a \cdot b$ , $2 \le a \le b < K+1$.

apply induction hypothesis.

Scanned by CamScanner

One interesting Example (Postage stamp problem)

2 types of stamps → 4-cent, 5-cent.

make a postage of n cents, $n \geq 12$.

a, b be two integers.

$\gcd(a, b) = 1$.

Linear Diophantin equation.

$ax + by = n$. ; $x, y > 0$.

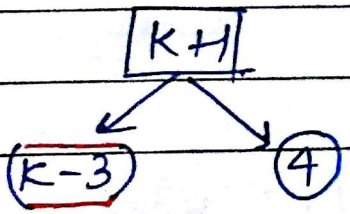
n is feasible if $n > ab - a - b$.

proof → {1. (Strong) induction proof}.

Basis step → P(12) is true.

Inductive step → P(12), P(13), ---, P(K) is true. (Assume).

Claim. → P(K+1) is True.




$K - 3 \geq 12 \Rightarrow K \geq 15$

{induction hypothesis holds for $K \geq 15$}.

so basis step must be.

P(12), P(13), P(14), P(15)

P(12) = 4×3

P(13) = 4×2 + 5×1

P(14) = 4×1 + 5×2

P(15) = 5×3.

proof (weak induction).

Basis step. → P(12) is True. $12 = 3 \times 4$.

Inductive step. → Assume P(K) is True.

Scanned by CamScanner

Claim → P(k+1) is True.

case 1 → at least one 4-cent stamp is used to form postage of (k) cents, $k \geq 12$.

case 2 → no 4-cent used to form k-cent postage.

$15 = 3 \times 5$, $16 = 4 \times 4$

Example → $|S| = n$, S is a finite set.

Then $|P(S)| = 2^n$ use mathematical induction.

$\emptyset$, $\{\emptyset\}$

$|\emptyset| = 0$

$|\{\emptyset\}| = 1$.

power set $P(\emptyset) = \{\emptyset\}$.

- S → non-empty.
  at least two subsets.
  $S \subseteq S$, $\emptyset \subseteq S$.
- $\emptyset$
  ↳ only one subset $\emptyset$.

find $P(P(\emptyset))$ =?, $P(P(P(\emptyset)))$ =?

Solution → Basis step → $S = \emptyset$.

$|S| = 0$.

$P(S) = \{\emptyset\}$., $|P(S)| = 1 = 2^0$

P(0) is True.

Inductive step. → Assume that P(n) is True.

claim → P(n+1) is true.

let T be any set, $|T| = n+1$

$a \in T$

$S = T - \{a\}$. $\Rightarrow |S| = n$.

Scanned by CamScanner