Def. Proposition

A statement that is either true or false, but not both.

Ex. "Today is Tue" } propositions
$1+3=13$

"What is your name?" } not propositions
$1+x=y+2$

* Use symbols $p, q, r, s, \ldots$ to denote propositions

* Compound proposition: Connect propositions using logical operators

* Truth table: display truth value of propositions

p	q	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \to q$
T	T	T	T	F	T
T	F	F	T	T	F
F	T	F	T	T	T
F	F	F	F	F	T

* Converse of $p \to q$ is $q \to p$

* contrapositive of $p \to q$ is $\neg q \to \neg p$

* Biconditional $p \leftrightarrow q \iff (p \to q) \wedge (q \to p)$

↑ Logically equivalent

Def. Tautology
Compound proposition that is always true

Def. Contradiction
compound proposition that is always false.

Ex. $p \vee (\neg p)$ tautology
$p \wedge (\neg p)$ contradiction

Logical Equivalences

1. Identity law
$p \wedge T \iff p$
$p \vee F \iff p$

2. Domination law
$p \vee T \iff T$
$p \wedge F \iff F$

3. Idempotent "
$p \wedge p \iff p$
$p \vee p \iff p$

4. Double negation $\neg(\neg p) \Leftrightarrow p$

5. Commutative $p \vee q \Leftrightarrow q \vee p$

$p \wedge q \Leftrightarrow q \wedge p$

6. Associative $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$

$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$

7. Distributive $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$

$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$

8. DeMorgan $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$

$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$

9. Misc $p \vee \neg p \Leftrightarrow T$

$p \wedge \neg p \Leftrightarrow F$

$p \rightarrow q \Leftrightarrow \neg p \vee q$

Aqil at 1/21/2021 10:01 AM

Ex. Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent.

$\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg(\neg p \wedge q)$

$\Leftrightarrow \neg p \wedge (p \vee \neg q)$

$$\Leftrightarrow (\neg p \wedge p) \vee (\neg p \wedge \neg q)$$
$$\Leftrightarrow \quad F \quad \vee (\neg p \wedge \neg q)$$
$$\Leftrightarrow \quad \neg p \wedge \neg q$$

Ex Determine if $\neg(p \wedge (p \to q)) \to \neg q$ is tautology?

$$\neg(p \wedge (p \to q)) \to \neg q \Leftrightarrow (p \wedge (p \to q)) \vee \neg q$$
$$\Leftrightarrow \neg q \vee (p \wedge (p \to q))$$
$$\Leftrightarrow (\neg q \vee p) \wedge (\neg q \vee (p \to q))$$
$$\Leftrightarrow (\neg q \vee p) \wedge (\neg q \vee (\neg p \vee q))$$
$$\Leftrightarrow (\neg q \vee p) \wedge (T \vee \neg p)$$
$$\Leftrightarrow (\neg q \vee p) \wedge T$$
$$\Leftrightarrow \neg q \vee p$$
$$\Leftrightarrow q \to p \quad \text{not tautology}$$

* The Statement "$x > 5$" is not a proposition.

* Proposition function $P(x) =$ "$x > 5$"

$P(2)$ is False
$P(100)$ " True

* We can have proposition function with multiple variables. $Q(x,y)$ = "$x + 1 = y$"

$Q(1,1)$ is False
$Q(10,11)$ " True

* Using quantifiers to assign values to the variables in the proposition function

Quantifiers: universal $\forall$; existential $\exists$

When using quantifiers we need to define the universe of discourse.

Def. The universal quantification of $P(x)$ is the propositional "$P(x)$ is true for all x in the universe of discourse"

Assume universe of discourse = $\{x_1, x_2, \ldots, x_n\}$

$$\forall x\, P(x) = P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n)$$

$$= \bigwedge_{i=1}^{n} P(x_i)$$

Def. The existential quantification of $P(x)$ is the propositional "$P(x)$ is true if there exist an element x in the universe of discourse

$\exists$ P(x) is true"

$$\exists x\, P(x) = P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n)$$

$$= \bigvee_{i=1}^{n} P(x_i)$$

Ex. Let $P(x)$ = "$x + 1 > 0$"

if universe of discourse is $\mathbb{R}$
$\forall x\, P(x)$ is False
$\exists x\, P(x)$ " True

Aqil at 1/24/2021 10:02 AM

Same $P(x)$ = "$x + 1 > 0$"

if universe of discourse is $\mathbb{Z}^+$
$\forall x\, P(x)$ is True

Expressing Statements using proposition functions

Let $F(x, y)$ = "y is ther father of x"

* Express the statement "Ali is the father of Bilal"

F(Bilal, Ali)

* "Ali is not father of Ahmad" $\neg F(\text{Ahmad}, \text{Ali})$

* "Everyone has a father" $\forall x \exists y\ F(x,y)$
  universe of discourse is all humans

* "Everyone has a single father"

$$\forall x \exists y \forall z\ F(x,y) \wedge ((z \neq y) \rightarrow \neg F(x,z))$$

for every person x, there is another person y ∋ y is father of x and if z is a person other than y then z is not father of x.

* "Everyone has a father and a mother"

Let $M(x,y)$ = "y is the mother of x"

$$\forall x \exists y \exists z\ F(x,y) \wedge M(x,z)$$

Another way to express the statement
Let $F(x)$ = "x has a father"
$M(x)$ = "x has a mother"

$$\forall x\ F(x) \wedge M(x)$$

* Multiple quantifiers, the order is important

Let $A(x,y)$ = "$x+y=0$"

$\forall x \forall y\ A(x,y) = \forall y \forall x\ A(x,y)$ False

$\exists x \exists y\ A(x,y) = \exists y \exists x\ A(x,y)$ True

$\underbrace{\forall x \exists y\ A(x,y)}_{\text{True}} \neq \underbrace{\exists y \forall x\ A(x,y)}_{\text{False}}$

* Negation of quantifiers

$\neg(\forall x\ P(x)) \Leftrightarrow \exists x\ (\neg P(x))$

$\neg(\exists x\ P(x)) \Leftrightarrow \forall x\ (\neg P(x))$

Let $P(x)$ = "x knows Arabic"

$\neg P(x)$ = "x does not know Arabic"

$\forall x\ P(x)$ = "Everyone knows Arabic"

$\neg(\forall x\ P(x))$ = "Someone does not know Arabic"

$\exists x\ P(x)$ = "Someone knows Arabic"

$\neg(\exists x\ P(x))$ = "No one knows Arabic"

All above assume Universe of discourse = Students in the classroom

Sets: a collection of objects

* each object is an element
* order of objects has no significance

Ex. Set $A = \{1, \text{car}, \square\}$

↑ element

$\text{car} \in A$

$2 \notin A$

Set $P = \{2, 3, 5, 7, 11, 13\}$

$= \{x \mid x \text{ is prime} < 15\}$

Set $E = \{100, 102, 104, \ldots, 200\}$

$= \{x \mid x \text{ is even integer between 100 and 200}\}$

Set $B = \{1, 2, \{3,4\}, 5, \{5\}\}$

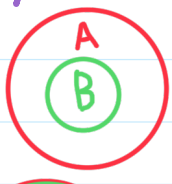
$1 \in B$ $\quad \{3,4\} \in B$

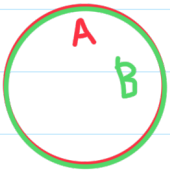
Empty set (set with no elements) $= \{\} = \emptyset$

* Subset: $A \subset B$ proper subset

$A \subseteq C$ subset

$\forall x \, (x \in A \rightarrow x \in C)$





* Two sets are identical iff each set is a subset

of the other.

Ex To show sets $A = B$ ① show $A \subseteq B$ ② show $B \subseteq A$

* cardinality of a set = # of elements in the set. Denoted $|A|$

Ex $A = \{1, 2, 3, \{3,4\}, 5, \{6\}\}$ $|A| = 6$

$1 \in A$
$3 \in A$
$\{3,4\} \in A$
$4 \notin A$
$\emptyset \notin A$

$\emptyset \subseteq A$
$1 \not\subseteq A$
$\{3,4\} \not\subseteq A$
$\{\{3,4\}\} \subseteq A$

* Powerset: set of all subsets of a set.

Ex. Let $A = \{1,2,3\}$

Powerset $P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

In general $|P(A)| = 2^{|A|}$

Ex $B = \{1, \{2\}\}$
$P(B) = \{\emptyset, \{1\}, \{\{2\}\}, \{1, \{2\}\}\}$

Ex $P(\emptyset) = \{\emptyset\}$ $|\emptyset| =$ zero
$|P(\emptyset)| = 1$

Ex $P(\phi) = \{\phi\}$ $\quad |\phi| = \text{zero}$

$|P(\phi)| = 1$

$P(P(\phi)) = \{\phi, \{\phi\}\}$

* Cartesian product of sets is a set of ordered tuples

$$A \times B = \{(x,y) \mid x \in A \wedge y \in B\}$$

pair or 2-tuple

Ex Let $A = \{1,2,3\}$, $B = \{a,b\}$

$$A \times B = \{(1,a),(1,b),(2,a),(2,b),(3,a),(3,b)\}$$

$$\neq B \times A$$

$$A_1 \times A_2 \times A_3 = \{(x,y,z) \mid x \in A_1 \wedge y \in A_2 \wedge z \in A_3\}$$

3-tuple

$$|A \times B| = |A| \cdot |B|$$

Aqil at 1/28/2021 10:03 AM

* Note $A \times \phi = \phi$

Set Operations

① ② ③ ④

④ Complement $\bar{A} = \{x \mid x \notin A\}$

③ Difference $A - B = \{x \mid x \in A \wedge x \notin B\}$

② Intersection $A \cap B = \{x \mid x \in A \wedge x \in B\}$

$\cup$ Union

$A \cup B = \{x \mid x \in A \vee x \in B\}$

Intersection $A \cap B = \{x \mid x \in A \wedge x \in B\}$

$x \notin D$

U = Universal Set المجموعة الكلية

Set Identities

① Identity law $A \cup \phi = A$

$A \cap U = A$

② Domination law $A \cap \phi = \phi$

$A \cup U = U$

③ Idempotent " $A \cup A = A \cap A = A$

④ Double complement $\bar{\bar{A}} = A$

⑤ Commutative law $A \cup B = B \cup A$

$A \cap B = B \cap A$

④ Associative " $(A \cup B) \cup C = A \cup (B \cup C)$

$(A \cap B) \cap C = A \cap (B \cap C)$

⑤ Distributive " $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

⑥ DeMorgan " $\overline{A \cup B} = \bar{A} \cap \bar{B}$

$\overline{A \cap B} = \bar{A} \cup \bar{B}$

Generalized DeMorgan $\overline{A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n} = \bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \cap \cdots \cap \bar{A}_n$

or $\overline{\bigcup_{i=1}^{n} A_i} = \bigcap_{i=1}^{n} \bar{A}_i$

Similarly, $\overline{\bigcap_{i=1}^{n} A_i} = \bigcup_{i=1}^{n} \bar{A}_i$

Ex. Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$

(1) Show $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$

Assume $x \in \overline{A \cap B}$

$\Rightarrow x \notin A \cap B$

$\Rightarrow x \notin A \vee x \notin B$

$\Rightarrow x \in \bar{A} \vee x \in \bar{B}$

$\Rightarrow x \in \bar{A} \cup \bar{B}$

(2) show $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$

assume $x \in \bar{A} \cup \bar{B}$

$\Rightarrow x \in \bar{A} \vee x \in \bar{B}$

$\Rightarrow x \notin A \vee x \notin B$

$\Rightarrow x \notin A \cap B$

$\Rightarrow x \in \overline{A \cap B}$

We can also prove it using Set building notation

$\overline{A \cap B} = \{ x \mid x \notin A \cap B \}$

$$= \{x \mid \neg(x \in A \cap B)\}$$

$$= \{x \mid \neg(x \in A \vee x \in B)\}$$

$$= \{x \mid x \notin A \wedge x \notin B\}$$

$$= \{x \mid x \in \bar{A} \wedge x \in \bar{B}\}$$

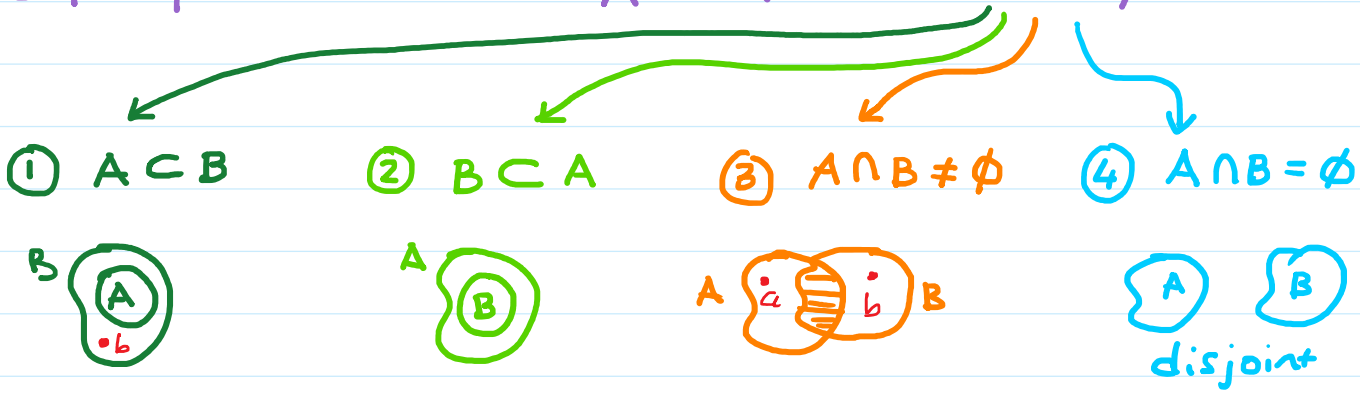
$$= \{x \mid x \in \bar{A} \cap \bar{B}\}$$

Problem

Given sets A, B, C such that

$$\left.\begin{aligned} A \cup C &= B \cup C \\ A \cap C &= B \cap C \end{aligned}\right\}$$ can we conclude that must $A = B$?

Proof by contradiction. Assume that $A \neq B$,



Aqil at 2/2/2021 10:07 AM

case #1. Let $B = A \cup \{b\} \ni b \notin A$.

then, $A \cup C = B \cup C \Rightarrow b \in C$ otherwise no equality

$A \cap C = B \cap C \Rightarrow b \notin C$ " " "

So, $A \not\subset B$

case #2. Similar to case #1. So, $B \not\subset A$

case #3. Let $A = \{\square, a\}$, $B = \{\square, b\}$ such that $\square$ is common to sets A, B; and $a \notin B$, $b \notin A$.

then,

$$A \cup C = B \cup C \Rightarrow a \in C \text{ and } b \in C$$
$$A \cap C = B \cap C \Rightarrow a \notin C \text{ and } b \notin C$$

∴ so, we cannot have $A \cap B \neq \emptyset$ and satisfy both statements.

case #4. A, B disjoint.

then,

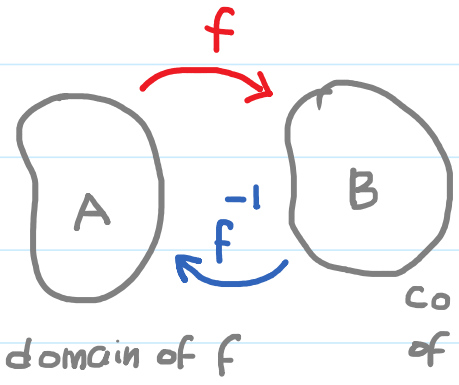
$$A \cup C = B \cup C \Rightarrow A \subset C \text{ and } B \subset C$$
$$A \cap C = B \cap C \Rightarrow A \not\subset C \text{ and } B \not\subset C$$

So, can't have A, B disjoint and satisfy both statements.

Therefore, $A \neq B$ fails and thus $A = B$.

Functions

Def. Let A, B be sets. Function from A to set B is an assignment of one element of B to each element of A.



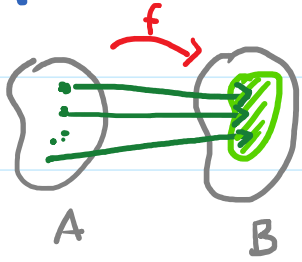
$f: A \to B$

$f(a) = b$

image of a under f

pre-image of b under f

Range of f: set of all images of A, $\{f(x) \mid \forall x \in A\}$



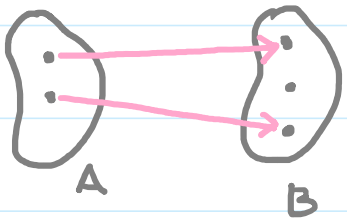
range of f

Types of functions

- 1-1
- Onto
- Neither
- 1-1 Correspondance

Def. f is 1-1 iff $f(x) = f(y) \Leftrightarrow x = y$ for $\forall x, y$ in the domain.

Also, $f(x) \neq f(y) \Leftrightarrow x \neq y$.

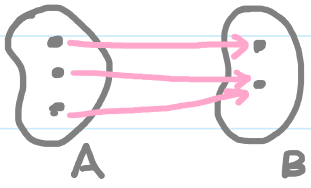


each $b \in B$ receives at most 1 arrow

$|A| \leq |B|$

Def. $f: A \to B$ is onto iff $\forall b \in B \ \exists a \in A \ni f(a) = b$.

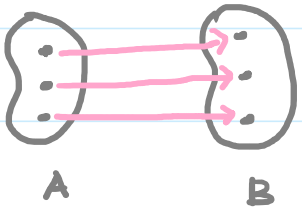
i.e. all elements of B is an image of some elements in set A.



each $b \in B$ receives at least 1 arrow

$|A| \geq |B|$

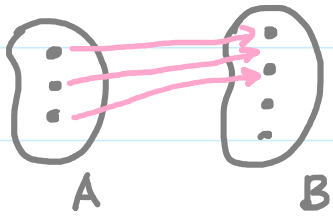
Def. f is 1-1 correspondance if f is both 1-1 and onto.



each $b \in B$ receives exactly 1 arrow.

$|A| = |B|$

Def. f is neither, if f is not 1-1 and not onto.



Def. Let $f: A \to B$ be 1-1 correspondance, then the inverse of f is $f^{-1}: B \to A \ni a = f^{-1}(b)$ where $b = f(a)$.

NOTE: only in case 1-1 correspondance each element has an inverse, otherwise we say f is not invertible.

Def. Let $f: A \to B$, and $g: B \to C$. Then the composition of f and g is defined as

$(g \circ f)(x) = g(f(x))$

$(f \circ g)(x)$ don't have

Ex Assume $f: \mathbb{R} \to \mathbb{R}$ and $g: \mathbb{R} \to \mathbb{R}$

Let $f(x) = 3x + 2$

$g(x) = \sqrt{x-1}$

$$(f \circ g)(x) = f(g(x))$$
$$= f(\sqrt{x-1})$$
$$= 3\sqrt{x-1} + 2$$

$$(g \circ f)(x) = g(f(x))$$
$$= g(3x+2)$$
$$= \sqrt{(3x+2)-1} = \sqrt{3x+1}$$

Sequences

Def. Sequence is a function $f: A \to S$ ∋ $A \subset \mathbb{Z}$

usually A is a set $\{0,1,2,\ldots\}$ or $\{1,2,3,\ldots\}$

* a_n denote image of integer n

index

term

Ex. Sequence $\{a_n\}$ ∋ $a_n = 1/n$ is sequence $\{1, 1/2, 1/3, \ldots\}$

Ex. Sequence $\{b_n\}$ ∋ $b_n = 2n$ is sequence $\{0, 2, 4, 6, \ldots\}$

b_0 b_1 b_2 b_3

Arithmetic sequence: difference between consecutive terms is constant

Geometric sequence: ratio between two consecutive terms is constant.

Ex. Consider the sequence $\{6, 11, 16, 21, \ldots\}$

next term = 26

Ex. Consider the sequence $\{a_n\}_{n \geq 1} = \{7, 13, 19, 25, \ldots\}$

$d = 6$ 6 6

Ex. Consider the sequence $\{a_n\}_{n\geq 1} = \{7, 13, 19, 25, \ldots\}$

a_1 a_2 a_3 a_4

General Formula for sequence

$$a_n = a_1 + d(n-1) \qquad n \geq 1$$

Here,

$$a_n = 7 + 6 \times (n-1) = 6n + 1$$

Ex. Assume a sequence $a_{50} = 102$, $a_{51} = 105$,

$a_{52} = 108$, $a_{53} = 111, \ldots$

Find: ① What is a_{200}?

② Index of term that is > 1000 and the previous term is < 1000

First, we want Formula for the sequence

$$a_n = a_1 + d(n-1)$$

$$a_{51} = 105 = a_1 + 3 \times 50 \Rightarrow a_1 = -45$$

$$\therefore a_n = -45 + 3(n-1)$$

$$= -48 + 3n$$

① $a_{200} = -48 \times 3 \times 200 = 552$

② Find index i ∋ $a_i > 1000$ and $a_{i-1} < 1000$

$$a_i = -48 + 3i > 1000$$

$$\Rightarrow i = \lceil 1048 \rceil = 350$$

$$\Rightarrow \quad i = \left\lceil \frac{1048}{3} \right\rceil = 350$$

Check $a_{349} = 999$, $a_{350} = 1002$

Ex. What is the next term of the sequence =

$\{1, 7, 25, 79, 241, 727, \ldots\}$

a_1 a_2 a_3 a_6

Look at ratios. $\frac{25}{7} = 3.57$, $79/25 = 3.16$

$241/79 = 3.05$, $727/241 = 3.02$

We see ratio $\longrightarrow 3$

This means a_n has 3^n term.

n	1	2	3	4	5
3^n	3	9	27	81	243
a_n	1	7	25	79	241

$\therefore a_n = 3^n - 2$, where $n \geq 1$.

So next term $a_7 = 3^7 - 2 = 2185$.

Ex. What is next term of the sequence

$\{4, 5, 7, 11, 19, 35, 67, 131, \ldots\}$

Ratios: $5/4 = 1.25$, $7/5 = 1.4$, $11/7 = 1.57$

$19/11 = 1.73$, $35/19 = 1.84$, $67/35 = 1.91$

in general ratio $\to 2$

$\therefore$ formula of a_n will have 2^n.

n	0	1	2	3	4
2^n	1	2	4	8	16
a_n	4	5	7	11	19

Thus $a_n = 2^n + 3$ for $n \geq 0$

next term $a_8 = 2^8 + 3 = 259$

Aqil at 2/9/2021 10:02 AM

Summation

Given a sequence $\{a_1, a_2, \ldots, a_n, \ldots\}$ we can sum the terms $\sum_{i=1}^{n} a_i$ or $\sum_{i=m}^{n} a_i$

↑ Summation index (always integer)

$$\sum_{i=1}^{n} C = C + C + \cdots + C = n \times C$$

$$\sum_{i=1}^{n} c = c + c + \cdots + c = n \times c$$

$$\sum_{i=m}^{n} c = c + c + \cdots + c = (n - m + 1) \times c$$

$$\sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n = \frac{1}{2} n(n+1)$$

Proof Let $S = 1 + 2 + 3 + \cdots + n$

$S = n + (n-1) + (n-2) + \cdots + 1$

($1 = n+1$, $2 = n+1$, $3 = n+1$, $n = n+1$)

$2S = n \times (n+1)$

$\therefore S = \frac{1}{2} n(n+1)$

Add $1 + 2 + 3 + \cdots + (m-1)$

$$\sum_{i=m}^{n} i = m + (m+1) + (m+2) + \cdots + n$$

Subtract $1 + 2 + 3 + \cdots + (m-1)$

$$= \sum_{i=1}^{n} i \quad - \quad \sum_{i=1}^{m-1} i$$

$$= \frac{1}{2} n(n+1) \quad - \quad \frac{1}{2} (m-1) \times m$$

$$= \frac{1}{2} (n^2 + n - m^2 + m)$$

$$\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{6} n(n+1)(2n+1)$$

$$\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{6} n(n+1)(2n+1)$$

$$\sum_{i=1}^{n} i^3 = 1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$$

$$\sum_{i=0}^{n} ar^i = a + ar + ar^2 + \cdots + ar^n = a\left(\frac{r^{n+1} - 1}{r-1}\right)$$

Proof Let $S = a + ar + ar^2 + \cdots + ar^n$ ①

$r \times S = ar + ar^2 + ar^3 + \cdots + ar^{n+1}$ ②

② − ① $= ar^{n+1} - a$

$(r-1) \times S = a(r^{n+1} - 1)$

$\therefore S = \dfrac{a(r^{n+1} - 1)}{r-1}$ $\quad r \neq 1$

$$\sum_{i=m}^{n} ar^i = \sum_{i=0}^{n} ar^i - \sum_{i=0}^{m-1} ar^i$$

$$= a\left(\frac{r^{n+1} - 1}{r-1}\right) - a\left(\frac{r^m - 1}{r-1}\right) = a\left(\frac{r^{n+1} - r^m}{r-1}\right)$$

$\sum_{}^{n} \sum_{}^{m} a_{..}$

Double Summation $\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}$

$\sum_{i=1}^{n}\left(\sum_{j=1}^{m} c\right)$ Always start with innermost Σ $= \sum_{i=1}^{n} cm = c \cdot m \cdot n$

$\rightarrow = cm$

$\sum_{i=1}^{n}\left(\sum_{j=1}^{m} i\right) = mi = \sum_{i=1}^{n} mi = \frac{1}{2}mn(n+1)$ (constant)

$\sum_{i=1}^{n}\left(\sum_{j=1}^{m} j\right) = \frac{1}{2}m(m+1) = \sum_{i=1}^{n} \frac{1}{2}m(m+1) = \frac{1}{2}nm(m+1)$

$\sum_{i=1}^{n}\left(\sum_{j=i}^{m} i\right) = (m-i+1) \times i = mi - i^2 + i$

$= \sum_{i=1}^{n} (mi - i^2 + i)$

$= \sum_{i=1}^{n} mi - \sum_{i=1}^{n} i^2 + \sum_{i=1}^{n} i$

$\sum_{i=1}^{n} i = \frac{1}{2}n(n+1)$

$\sum_{i=1}^{n} mi = \frac{1}{2}mn(n+1)$

$\sum_{i=1}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$

$= \frac{1}{2}n(n+1)\left[m - \frac{2n+1}{3} - 1\right]$

Aqil at 2/11/2021 10:03 AM

Some other ways to express summation

$$\sum_{p \text{ prime} < 20} p = 2+3+5+7+11+13+17+19$$

$$\sum_{k \text{ is odd} < 30} k = 1+3+5+\cdots+29$$

$$\prod_{i=1}^{n} c = c \times c \times c \times \cdots \times c = c^n$$

$$\prod_{i=1}^{n} i = 1 \times 2 \times 3 \times \cdots \times n = n!$$

$$\sum_{i=1}^{n} \prod_{j=1}^{i} j = \sum_{i=1}^{n} i! = 1! + 2! + 3! + \cdots + n!$$

Proof Techniques

Any theorem takes the form "if p then q" $p \to q$

p: proposition / hypothesis

q: conclusion

Proof methods
- Induction
- counter example
- proof by cases
- Direct proof
- Indirect proof
- proof by Contradiction

1 Direct Proof. $p \to q$

Assume p is true

accordingly, we show that q is true

Show that if [n is odd] (p) then [n^2 is odd] (q)

p is True

Assume n is odd. Let $n = 2k+1$ for some $k \in \mathbb{Z}$.

Then
$$n^2 = (2k+1)^2$$
$$= 4k^2 + 4k + 1$$
$$= 2(2k^2 + 2k) + 1$$
($2k^2 + 2k$: integer)
$$= \text{odd}$$

q is true

2 Indirect proof $p \to q \iff \neg q \to \neg p$

Show that if [n^2 is even] (p) then [n is even] (q)

$\neg q$: Assume n is odd. Let $n = 2k+1$ for $k \in \mathbb{Z}$

then,
$$n^2 = (2k+1)^2$$
$$= 2(2k^2 + 2k) + 1$$
$$= 1$$

$\neg p$

$= 2(2k^2 + 2k) + 1$

$=$ odd

[3] Proof by contradiction $p \to q \iff \neg p \to F$

Show that $\sqrt{2}$ is irrational — p

$\neg p$: Assume $\sqrt{2}$ is rational.

Let $\sqrt{2} = a/b \ \ni \ a, b \in \mathbb{Z}$ and assume it is in simplest form (لا يوجد اختزال)

squaring, $a^2 = 2b^2$

$= \text{even} \Rightarrow$ a is even.

Let $a = 2k$. So,

$a^2 = (2k)^2 = 2b^2 \Rightarrow b^2 = 2k^2$

$= \text{even}$

$\Rightarrow$ b is even

contradiction

$\therefore$ Our assumption was wrong. So $\sqrt{2}$ is rational.

Aqil at 2/14/2021 10:01 AM

In general, proof by contradiction

① $\neg p \to$ contradiction

② Assume p and $\neg q$

use indirect proof

$\neg q \to \neg p$ — Contradiction

Ex. Show that if $3n+2$ is odd (p) then n is odd (q)

Assume $3n+2$ is odd (p)

n " even $(\neg q)$

Let $n = 2k$ for $k \in \mathbb{Z}$.

Then $3n+2 = 3(2k)+2 = 2(3k+1) = \text{even}$ $(\neg p)$

4 Proof by cases

Assume $p = p_1 \vee p_2 \vee p_3 \vee \cdots \vee p_n$

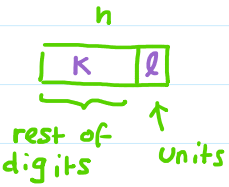
$p \to q \iff (p_1 \to q) \wedge (p_2 \to q) \wedge \cdots \wedge (p_n \to q)$

Ex Show that any integer ending with 2 cannot be perfect square.

XXXX2 ← خانة الآحاد

مربع كامل 1, 4, 9, 16, 25, ...

Idea: Split integer n into 2 parts



$n = 10K + \ell$

بقية الأقسام ← ← خانة الآحاد

$n^2 = (10K + \ell)^2 = 100K^2 + 20K\ell + \ell^2$

$= 10(10K^2 + 2K\ell) + \ell^2$

This means the unit digit of n^2 is fully dependent on the unit digit of ℓ^2

Now $0 \le \ell \le 9$

case 1. $\ell = 0$. then $\ell^2 = 0$

case 2. $\ell = 1$, " $\ell^2 = 1$

case 3. $\ell = 2$, " $\ell^2 = 4$

case 4. $\ell = 3$, " $\ell^2 = 9$

case 5. $\ell = 4$, " $\ell^2 = 16$

Case 6. $\ell = 5$, " $\ell^2 = 25$

case 7. $\ell = 6$, " $\ell^2 = 36$

Case 8. $\ell = 7$, " $\ell^2 = 49$

case 9. $\ell = 8$, " $\ell^2 = 64$

case 10. $\ell = 9$, " $\ell^2 = 81$

Square of an integer ends in 0, 1, 4, 5, 6, 9

5 Counter Example. مثال مناقض

Used to disprove a theorem or a statement.

Ex. "Any integer ending with 1 cannot be

a perfect square"

counter example. $121 = 11^2$

Ex. "All prime integers are odd"

2 is even integer and is prime.

Aqil at 2/16/2021 10:02 AM

Mathematical Induction

- Weak induction
  - Base case: Show $P(1)$ is True
  - Inductive case: Assume $P(n)$ is True; Show $P(n) \to P(n+1)$
  - } $\forall n\ P(n)$
- Strong induction
  - Base case
  - Inductive case: Assume $P(1) \wedge P(2) \wedge \dots \wedge P(n)$ are True; then show $P(n+1)$ is True

Weak Induction: $[P(1) \wedge \forall n\ P(n) \to P(n+1)] \to \forall n\ P(n)$

Ex. Use induction to show $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$

Let $P(n) =$ " $\sum_{k=1}^{n} k = \frac{1}{2}n(n+1)$ "

Base case $(n=1)$

LHS of $P(1) = \sum_{k=1}^{1} k = 1$

RHS of $P(1) = \frac{1}{2} \times 1 \times 2 = 1$

} $P(1)$ is True

Inductive case

Assume $P(n)$ is True for some $n \geq 1$. We show that $P(n+1)$ is also True.

$$\text{LHS of } P(n+1) = \sum_{k=1}^{n+1} k = \left(\sum_{k=1}^{n} k\right) + (n+1)$$

$$= \frac{n(n+1)}{2} \quad \text{by induction hypothesis}$$

$$= n(n+1) \cdot (n+1)$$

hypothesis

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

$$= (n+1)\left(\frac{n}{2} + 1\right)$$

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

$$= \text{RHS of } P(n+1)$$

Ex. Use induction to show $\sum_{k=m}^{n} r^k = \frac{r^{n+1} - r^m}{r-1}$

Let $P(n) = "\sum_{k=m}^{n} r^k = \frac{r^{n+1} - r^m}{r-1}"$

Base case $(n = m)$

LHS of $P(m) = \sum_{k=m}^{m} r^k = r^m$

RHS of $P(m) = \frac{r^{m+1} - r^m}{r-1} = \frac{r^m(r-1)}{r-1} = r^m$

$\therefore P(m)$ is True

Inductive case

Assume $P(n)$ is True for some $n \geq m$.

We show that $P(n+1)$ is also True.

LHS of $P(n+1) = \sum_{k=m}^{n+1} r^k = \left(\sum_{k=m}^{n} r^k\right) + r^{n+1}$

$$= \frac{r^{n+1} - r^m}{r-1}$$

by induction hypothesis

$$= \frac{r^{n+1} - r^m}{r-1} + r^{n+1}$$

$$= r^{n+1}\left[\frac{1}{r-1} + 1\right] - \frac{r^m}{r-1}$$

$$= \frac{r}{r-1}$$

$$= \frac{r^{n+2}}{r-1} - \frac{r^m}{r-1}$$

$= \text{RHS of } P(n+1)$

Ex. Show that $n! > 2^n$ for $n \geq 4$

Base case $(n = 4)$

$4! = 24 > 2^4 = 16$

$\therefore$ base case is True.

Inductive case

Assume $n! > 2^n$ for some $n \geq 4$. We show it is true for next n.

$(n+1)! = (n+1) \times n! > 2^n$ by inductive hypothesis

$> (n+1) \times 2^n$

$> 2 \times 2^n = 2^{n+1}$

Aqil at 2/21/2021 10:05 AM

Ex. Let $H_k = 1 + 1/2 + 1/3 + \cdots + 1/k$

Show that $H_{2^n} \geq 1 + n/2$.

Let $P(n) =$ "$H_{2^n} \geq 1 + n/2$"

Base case $(n = 0)$

LHS $= H_{2^0} = H_1 = 1$

RHS $= 1 + 0/2 = 1$

$\}$ $P(0)$ is true

Inductive case

Assume $P(n)$ is true. We show $P(n+1)$ is true.

LHS $P(n+1) = H_{2^{n+1}} = \boxed{1 + 1/2 + 1/3 + \cdots + \frac{1}{2^n}} + \cdots + \frac{1}{2^{n+1}}$

$= H_{2^n} \geq 1 + n/2$ based on induction hypothesis

$$H_{2^{n+1}} \geq 1 + \frac{n}{2} + \left(\frac{1}{2^n+1} + \frac{1}{2^n+2} + \cdots + \frac{1}{2^{n+1}}\right)$$

$$H_{2^{n+1}} \geq 1 + \frac{n}{2} + \left(\frac{1}{2^n+1} + \frac{1}{2^n+2} + \cdots + \frac{1}{2^{n+1}}\right)$$

lower bound ?

= Smallest term x # terms

$$\frac{1}{2^n+1} + \frac{1}{2^n+2} + \frac{1}{2^n+3} + \cdots + \frac{1}{2^n+2^n}$$

$$\therefore H_{2^{n+1}} \geq 1 + \frac{n}{2} + \frac{1}{2^{n+1}} \times 2^n \quad \left(= \frac{1}{2}\right)$$

$$\geq 1 + \frac{n}{2} + \frac{1}{2} = 1 + \left(\frac{n+1}{2}\right) = \text{RHS } P(n+1)$$

Aqil at 2/23/2021 10:04 AM

Strong Induction

$$[P(1) \wedge P(2) \wedge \cdots \wedge P(n) \rightarrow P(n+1)] \rightarrow \forall n \; P(n)$$

Ex. Show that any number $n \geq 8$ can be written as sum of bunch of 3's and 5's.

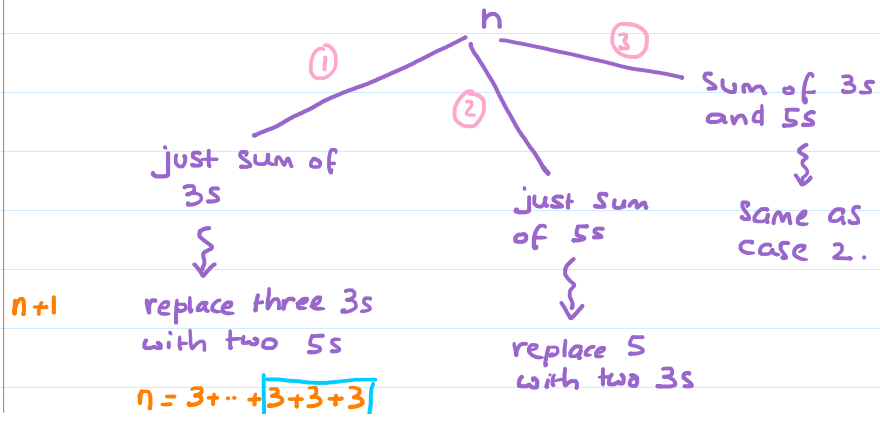
Let $P(n)$ = "n can be written as sum of 3s and 5s".

Base case ($n = 8$)

$P(8)$ is True since $8 = 3 + 5$

Inductive case

Assume $P(k)$ is true for $k = 8, 9, 10, \ldots, n$. We Show $P(n+1)$ is also true.



with two 5s

$n = 3 + \cdots + 3+3+3$

$n+1 = 3 + \cdots + 5+5$

replace 5 with two 3s

$n = 5 + 5 + \cdots + 5$

$n+1 = 3+3+5+\cdots+5$

Integers and Division

Def. integers a, b and $a \neq 0$. b يقسم a

Denote a divides b by $a \mid b$.

" a does not divide b by $a \nmid b$

b لا يقسم a

note $a \mid b \Rightarrow \exists$ integer $x \Rightarrow b = ax$

Ex $3 \mid 9$, $4 \mid 12$, $7 \mid 35$

$3 \nmid 10$, $4 \nmid 10$, $7 \nmid 36$

Th integers a, b, c then

- if $a \mid b$ and $a \mid c$ then $a \mid (b+c)$
- if $a \mid b$ and $b \mid c$ then $a \mid c$.
- if $a \mid b$ then $a \mid bc$ for any $c \in \mathbb{Z}$

Proof Suppose $a \mid b$ and $a \mid c$ then $\exists$ integers $x, y \ni b = ax$, and $c = ay$.

$\therefore b + c = ax + ay = a(x+y)$

thus $a \mid (b+c)$

Def. A positive integer $p > 1$ is prime $\Leftrightarrow$ the only positive factors are 1 and p. (integer)

NOTE: not prime is called "composite"

Ex. 7 is prime. 9 is not prime since $3 \mid 9$

Th Every positive integer can be written uniquely as a product of primes.

Ex. $9 = 3 \times 3$

$10 = 2 \times 5$

$100 = 2 \times 2 \times 5 \times 5$

Aqil at 2/28/2021 10:04 AM

Th if n is composite, then n has a prime divisor $\leq \sqrt{n}$

Proof.

n composite $\iff$ exist integers a, b where $1 < a \leq b < n \ni n = a \times b$.

I claim that either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

That is, can't have both a and $b > \sqrt{n}$ simultaneously for it leads to

$n = a \times b > \sqrt{n} \times \sqrt{n} = n$, a contradiction.

Th There are infinite number of primes.

Proof. Assume they are finite. Let these be: $p_1, p_2, \ldots, p_n$.

Define $x = (p_1 \times p_2 \times \cdots \times p_n) + 1$

Either x is prime or composite.

$p_1 \nmid x$, $p_2 \nmid x$, $p_3 \nmid x$, $\cdots$, $p_n \nmid x$

$\therefore$ x is prime $> p_n$.

Ex. 113 prime? YES.

$2 \nmid 113$, $3 \nmid 113$, $5 \nmid 113$, $7 \nmid 113$ stop since $11 > \sqrt{113}$

تحليل العدد إلى عواملة الأولية

Prime Factorization: finding all the prime factors that if multiplied results in the target integer.

Ex. Factor $7007 = 7 \times 7 \times 11 \times 13$ (unique factors)

$2 \nmid 7007$, $3 \nmid 7007$, $5 \nmid 7007$

$7 \mid 7007 \Rightarrow \frac{7007}{7} = 1001$

$7 \mid 1001 \Rightarrow \frac{1001}{7} = 143$

$7 \nmid 143$, $11 \mid 143 \Rightarrow \frac{143}{11} = 13$

Ex. Find prime factor of $9761 = 43 \times 227$

$2 \nmid 9761$, $3 \nmid 9761$, $5 \nmid 9761$, $7 \nmid 9761$,

$11 \nmid 9761$, $13 \nmid 9761$, $\ldots$, $41 \nmid 9761$

$43 \mid 9761 \Rightarrow \frac{9761}{43} = 227$ stop

this number is prime.

because $43 > \sqrt{227}$.

So, if 227 was not prime then we would had a prime factor $\leq 15 \simeq \sqrt{227}$.

Greatest Common Divisors & Least Common Multiple

Def. a, b integers $\neq 0$. Then the largest integer d $\ni$ $d|a$ and $d|b$ is called "greatest common divisor of a and b". القاسم المشترك الأكبر

Ex. Find $\gcd(24,36)$

Divisors of 24 : 1, 2, 3, 4, 6, 12, 24

" " 36 : 1, 2, 3, 4, 6, 9, 12, 18, 36

Def. Integers a, b are relatively prime if $\gcd(a,b)=1$.

Ex. $\gcd(5,9)=1$ 5, 9 are relatively prime

$\gcd(25,49)=1$ 25, 49 " " "

$\gcd(4,6)\neq 1$ 4, 6 are not rel. prime

Def. Integers $a_1, a_2, a_3, \ldots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j)=1 \quad \forall\, i \neq j$

Ex. Integers 10, 17, 21 are pairwise rel. prime.

gcd = 1 (17, 21)

gcd = 1 (10, 17)

gcd = 1 (10, 21)

Ex integers 10, 19, 24 are not pairwise rel. prime.

Ex integers 10, 19, 24 are not pairwise rel. prime.

gcd = 1

gcd = 1 gcd ≠ 1

each integer is written as unique product of primes

Th Let $a = \prod_{i=1}^{n} p_i^{\alpha_i}$, and $b = \prod_{i=1}^{n} p_i^{\beta_i}$ where $p_1, p_2, \ldots, p_n$ are primes and $\alpha_i, \beta_i \geq 0$.

Then

$$\gcd(a,b) = \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)}$$

Proof. Let $d = \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)}$.

To show d is the gcd(a,b) we need to show that it satisfies:

① $d \mid a$ and $d \mid b$

True since the power of each prime does not exceed the power of the same prime in either a or b.

② $\nexists\ d' > d \ni d' \mid a$ and $d' \mid b$.

True since increasing the power of any of the primes in d then either $d \nmid a$ or $d \nmid b$

Ex Find gcd(120, 500)

$120 = 2^3 \cdot 3 \cdot 5$ $\quad 500 = 2^2 \cdot 5^3$

$\gcd(120, 500) = 2^2 \times 3^0 \times 5^1 = 20$

Def. The least common multiple of positive integers a, b is the smallest positive integer which is divisible by both a and b. المضاعف المشترك الأصغر

Denoted $\text{lcm}(a, b)$

Th Given a, b then $\text{lcm}(a,b) = \prod_{i=1}^{n} p_i^{\max(\alpha_i, \beta_i)}$,

where p_i prime, $\alpha_i, \beta_i \geq 0$.

Proof. Let $\gamma = \prod_{i=1}^{n} p_i^{\max(\alpha_i, \beta_i)}$

To show γ is the $\text{lcm}(a,b)$ we show

① $a \mid \gamma$ and $b \mid \gamma$

② There does not exist $\gamma' < \gamma \ni a \mid \gamma'$ and $b \mid \gamma'$

Ex Find $\text{lcm}(120, 500)$

$120 = 2^3 \times 3 \times 5$ $\quad$ $500 = 2^2 \times 5^3$

$\text{lcm}(120, 500) = 2^3 \times 3^1 \times 5^3 = 3000$

Th $a, b > 0$ integers. Then

$$a \times b = \gcd(a,b) \times \text{lcm}(a,b)$$

Proof.

$$\gcd(a,b) \cdot \text{lcm}(a,b) = \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)} \times \prod_{i=1}^{n} p_i^{\max(\alpha_i, \beta_i)}$$

Proof:

$$\gcd(a,b)\cdot \operatorname{lcm}(a,b) = \prod_{i=1}^{n} p_i^{\min(\alpha_i,\beta_i)} \times \prod_{i=1}^{n} p_i^{\max(\alpha_i,\beta_i)}$$

$$= \prod_{i=1}^{n} p_i^{\min(\alpha_i,\beta_i)+\max(\alpha_i,\beta_i)}$$

$$= \prod_{i=1}^{n} p_i^{\alpha_i+\beta_i} = \prod_{i=1}^{n} p_i^{\alpha_i} \cdot \prod_{i=1}^{n} p_i^{\beta_i} = a \times b$$

Ex. $\gcd(120, 500) = 20$

$\operatorname{lcm}(120, 500) = 3000$

$120 \times 500 = 60000 = 20 \times 3000$

Modular Arithmetic

Def. Integers a, $m > 0$, we denote the remainder of a/m by $a \bmod m$.

* $a \bmod m = r \Rightarrow a = qm + r$

r: unique $0 \le r < m$

Ex $17 \bmod 5 = 2$ since $17 = 3 \times 5 + 2$

$-17 \bmod 5 = 3$ " $-17 = -4 \times 5 + 3$

Def. Integers a, b, $m > 0$, then

$a \equiv b \bmod m \Leftrightarrow m \mid (a - b)$

$a \equiv b \bmod m$: a is congruent to b modulo m

Ex $17 \equiv 5 \bmod 6$ since $6 \mid (17 - 5)$

$17 \not\equiv 5 \bmod 7$ " $7 \nmid (17 - 5)$

NOTE: $a \equiv b \bmod m \Leftrightarrow a \bmod m = b \bmod m$ (*)

$a \not\equiv b \bmod m \Leftrightarrow a \bmod m \neq b \bmod m$ (**)

Proof (*) $\Rightarrow$

$a \equiv b \bmod m \Rightarrow m \mid (a - b)$

$\Rightarrow \quad a - b = mk$

$\Rightarrow \quad a = b + mk$

$\Rightarrow \quad a \bmod m = (b + mk) \bmod m$

$= b \bmod m + mk \bmod m$ ($mk \bmod m = 0$)

$(**) \Leftarrow$

Given $a \bmod m \neq b \bmod m$

Let $\left.\begin{aligned} a &= mq_1 + r_1 \\ b &= mq_2 + r_2 \end{aligned}\right\} r_1 \neq r_2$ since

then,

$a - b = m(q_1 - q_2) + \underbrace{(r_1 - r_2)}_{\neq 0}$

$\therefore \quad m \nmid (a-b) \quad$ or $\quad a \not\equiv b \bmod m$

Th Let $m > 0$, then

$a \equiv b \bmod m \Leftrightarrow \exists$ integer $k \ni a = b + km$

Proof. $\Rightarrow$

$a \equiv b \bmod m \Rightarrow m \mid (a-b)$

$\Rightarrow \quad a - b = km \quad$ for some $k \in \mathbb{Z}$

$\Rightarrow \quad a = b + km$

Th Let $m > 0$ integer, if $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then $a + c \equiv b + d \bmod m$

$$a \times c \equiv b \times d \mod m$$

Proof.

$$a \equiv b \mod m \Rightarrow a = b + k_1 m$$
$$c \equiv d \mod m \Rightarrow c = d + k_2 m \quad \Big\} \; k_1 \neq k_2$$

Now,

$$a \times c = (b + k_1 m) \times (d + k_2 m)$$
$$= b \times d + \underbrace{(b k_2 + d k_1 + k_1 k_2)}_{\text{integer}} \times m$$

$$\therefore m \mid (a \times c - b \times d)$$
$$\Rightarrow ac \equiv bd \mod m$$

Th Let $a = bq + r$ $\ni$ a, b, q, r integer and $0 \leq r < b$ then $\gcd(a, b) = \gcd(b, r)$

Proof Assume $d \mid a$ and $d \mid b$ then

$d \mid (xa \pm yb) \Rightarrow x, y \in \mathbb{Z}$.

Let $x = 1$, and $y = q$, then $d \mid \underbrace{(a - bq)}_{= r} \Rightarrow d \mid r$

Means if $d \mid a$ and $d \mid b$ then $d \mid r$.

The common divisor of a, b, r is the same.

Euclidean Algorithm for gcd

Ex. Use Euclidean Algorithm to find gcd(287, 91)

← # ≥ 0 and < 91

$287 = \boxed{3} \times 91 + \boxed{14}$

$91 = \boxed{6} \times 14 + \boxed{7}$ ← gcd

$14 = \boxed{2} \times 7 + \boxed{0}$

Aqil at 3/9/2021 10:04 AM

Th if a, b positive integers then ∃ integers s and t

∋ gcd(a, b) = sa + bt.

This means we can express gcd of two numbers as a linear combination of both numbers.

Ex Express gcd(252, 198) as a linear combination of its arguments

① calculate gcd using Euclidean

$252 = \boxed{1} \times 198 + \boxed{54}$

$198 = \boxed{3} \times 54 + \boxed{36}$

$54 = \boxed{1} \times 36 + \boxed{18}$ ~ gcd

$36 = \boxed{2} \times 18 + \boxed{0}$

② Start from gcd and go backward

$18 = 54 - 1 \times 36$

$= 54 - 1 \times (198 - 3 \times 54)$

$= -1 \times 198 + 4 \times 54$

$= -1 \times 198 + 4 \times (252 - 1 \times 198)$

$= 4 \times 252 - 5 \times 198$

Thus

$$\gcd(252, 198) = 18 = 4 \times 252 - 5 \times 198$$

Lemma a, b, c positive integers $\ni \gcd(a, b) = 1$ and $a \mid bc$ then $a \mid c$.

Proof.

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

$= sa + tb$ (from Th.)

multiply both sides by c

$\Rightarrow \quad sac + tbc = c$

Now $a \mid sac$ and $a \mid tbc$

so $a \mid (\underbrace{sac + tbc}_{= c}) \quad \Rightarrow \quad a \mid c$

NOTE if $a \mid bc$ then $a \mid b$ or $a \mid c$ is false since it is possible that $a \nmid b$ and $a \nmid c$

Ex. $6 \mid 8 \times 9$ but $6 \nmid 8$ and $6 \nmid 9$

Lemma if p is prime and $p \mid a_1 \times a_2 \times \cdots \times a_n$ then $p \mid a_i$ for some i.

Th Let a, b, c, and $m > 0$ integers.

if $ac \equiv bc \mod m$ and $\gcd(c, m) = 1$

then $a \equiv b \mod m$.

Proof.

Given $ac \equiv bc \mod m \Rightarrow m \mid (ac - bc)$

$\Rightarrow m \mid c \times (a - b)$

But $m \nmid c$ since $\gcd(c, m) = 1$

therefore $m \mid (a - b) \Rightarrow a \equiv b \mod m$.

NOTE in general if $ac \equiv bc \mod m$ we can't cancel c from both sides unless it is relatively prime to m.

Th If a, m are relatively prime. Then $\exists$ a unique integer $\acute{a} < m \ni a \times \acute{a} \equiv 1 \mod m$.

($\acute{a}$ is called inverse of a in modulo m).

Proof.

Given $\gcd(a, m) = 1$

So $sa + tm = 1$ (from Th.)

$\equiv 1 \mod m$

but $tm \mod m = 0$, so $sa \equiv 1 \mod m$

↑ this is our inverse $\acute{a}$

Ex Find the inverse of 4 in modulo 7.

Since $\gcd(4,7)=1 \Rightarrow$ inverse exist

This inverse $= 2$ Since $2 \times 4 = 8 \equiv 1 \bmod 7$

Aqil at 3/11/2021 10:03 AM

Ex Find inverse of all numbers in modulo 7

No.	1	2	3	4	5	6
Inverse	1	4	5	2	3	6

Ex. Find inverse of all numbers in modulo 8

No.	1	2	3	4	5	6	7
Inverse	1	—	3	—	5	—	7

↑ No inverse since 2 and 8 are not relatively prime

Ex. What is the inverse of 25 in modulo 63

① Is 25 and 63 relatively prime? Yes $\Rightarrow$ inverse $\exists$

② Use Euclidean to calculate $\gcd(63, 25)$

③ Express gcd as linear combination.

$63 = \boxed{2} \times 25 + \boxed{13}$

$25 = \boxed{1} \times 13 + \boxed{12}$

$13 = \boxed{1} \times 12 + \boxed{1}$ ← gcd

$1 = 13 - 1 \times 12$

$= 13 - 1 \times (25 - 1 \times 13)$

$= -1 \times 25 + 2 \times 13$

$= -1 \times 25 + 2 \times (63 - 2 \times 25)$

$= 2 \times 63 \boxed{-5} \times 25$

-5 ← inverse of 25 in modulo 63

$-5 \equiv 58 \mod 63$

Check: $25 \times 58 = 1450 \equiv 1 \mod 63$

Ex Solve equation $22x \equiv 3 \mod 51$

This equation has unique solution since 22 and 51 are relatively prime

$x \equiv 3 \times \underbrace{(\text{inverse of } 22 \text{ in modulo } 51)}_{=7} \mod 51$

$\equiv 3 \times 7 \mod 51 = 21 \mod 51$

$x \equiv 21 \mod 51$

General solution $x = 21 + 51k \quad k \in \mathbb{Z}$

Ex Solve $5x^2 \equiv 3 \mod 9$

are relatively prime. We may have either two solutions or no solution

$x^2 \equiv 3 \times \underbrace{(\text{inverse of } 5 \text{ in modulo } 9)}_{=2} \mod 9$

$\equiv 6 \mod 9$

x	x^2	$x^2 \bmod 9$
1	1	1
2	4	4
3	9	0
4	16	7
5	25	7
6	36	0
7	49	4
8	64	1

no 6 $\Rightarrow$ no solution

Th Chinese Remainder Theorem (CRT)

Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime.

Then $x \equiv a_1 \mod m_1$

$x \equiv a_2 \mod m_2$

$\vdots$

$x \equiv a_k \mod m_k$

has a unique solution $0 \le x < \prod_{i=1}^{k} m_i$

Aqil at 3/14/2021 10:03 AM

Ex Solve

$x \equiv 2 \mod 3$ ($a_1 = 2$, $m_1 = 3$)

$x \equiv 3 \mod 5$ ($a_2 = 3$, $m_2 = 5$)

are pairwise relatively prime.

$x \equiv 3 \pmod 5$ (a_2, m_2)

$x \equiv 2 \pmod 7$ (a_3, m_3)

are pairwise relatively prime.

Let $m = m_1 \times m_2 \times m_3 = 3 \times 5 \times 7 = 105$

$M_1 = \frac{m}{m_1} = 35 \qquad M_2 = \frac{m}{m_2} = 21 \qquad M_3 = \frac{m}{m_3} = 15$

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod m$$

(y_1: inverse of M_1 in modulo m_1)

For y_1: $M_1 y_1 \equiv 1 \pmod{m_1} \Rightarrow 35 y_1 \equiv 1 \pmod 3 \Rightarrow y_1 = 2$

" y_2: $M_2 y_2 \equiv 1 \pmod{m_2} \Rightarrow 21 y_2 \equiv 1 \pmod 5 \Rightarrow y_2 = 1$

" y_3: $M_3 y_3 \equiv 1 \pmod{m_3} \Rightarrow y_3 = 1$

$x = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 \pmod{105}$

$= 233 \pmod{105}$

$= 23$

General Solution $x = 23 + 105k \qquad k \in \mathbb{Z}$

Th Fermat's Little Theorem

If p prime and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod p$

or $a^p \equiv a \pmod p$

NOTE: Converse is not true

Ex According to Fermat $6^{10} = 60466176 \equiv 1 \pmod{11}$

NOTE: Converse is not true

Ex According to Fermat $6^{10} = 60466176 \equiv 1 \bmod 11$

$9^{10} \equiv 1 \bmod 11$

Th Euler's Generalization

if a and n are relatively prime.

Then

$$a^{\phi(n)} \equiv 1 \bmod n,$$

where $\phi(n)$ is Euler's totient function.

= # of numbers $< n$ that are relatively prime to n.

Mathematically

$$\phi(n) = \left| \{x \mid 1 \le x < n \text{ and } \gcd(x,n) = 1\} \right|$$

Ex $\phi(12) = |\{1,5,7,11\}| = 4$

$\phi(15) = |\{1,2,4,7,8,11,13,14\}| = 8$

In general $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ $\exists$ $p_1, p_2, \ldots$ primes

then

$$\phi(n) = n\left(\frac{p_1-1}{p_1}\right)\cdot\left(\frac{p_2-1}{p_2}\right)\cdots\left(\frac{p_k-1}{p_k}\right)$$

$$= n \prod_{p \mid n} \left(\frac{p-1}{p}\right)$$

Ex. $12 = 2^2 \times 3 \Rightarrow \phi(12) = 12 \times \frac{1}{2} \times \frac{2}{3} = 4$

$15 = 3 \times 5 \Rightarrow \phi(15) = 15 \times \frac{2}{3} \times \frac{4}{5} = 8$

NOTE: $\phi(p) = p - 1$ where p is prime.

So,

$$a^{\phi(p)} = a^{p-1} \equiv 1 \bmod p \qquad \text{Fermat L. Th.}$$

Ex. Calculate $14^{100} \bmod 31 = ?$

Since 31 is prime we can use Fermat Th.

$14^{30} \equiv 1 \bmod 31.$

Cubing both sides, $(14^{30})^3 = 14^{90} \equiv 1^3 \bmod 31 = 1$

So,

$14^{100} = 14^{90} \times 14^{10} \bmod 31$ ($14^{90} = 1$)

$\equiv 14^{10} \bmod 31.$

Use repeated squaring

$14 \equiv 14 \bmod 31$

$14^2 = 196 \equiv 10 \bmod 31$

$14^4 = (14^2)^2 \equiv 10^2 \bmod 31 = 7$

$14^8 \equiv 7^2 \bmod 31 = 18$

Then,

$14^{10} = 14^8 \times 14^2 \equiv 18 \times 10 \bmod 31 = 25$

Thus $14^{100} \equiv 25 \mod 31$

Aqil at 3/16/2021 10:04 AM

Ex. What is the last two digits of 27^{1203}?

$27^{1203} = \underbrace{\ldots\ldots XX}_{\#\text{ digits} = 1722 \sim \lceil \log_{10} 27^{1203} \rceil}$ ← last two digits

Last two digits $= 27^{1203} \mod 100$

Can't use Fermat since 100 not prime.

Can we use Euler? Yes since 27 and 100 are rel. prime.

According to Euler, $27^{\phi(100)} = 40$

$\equiv 1 \mod 100$

$27^{1203} = 27^{1200} \times 27^3 = (27^{40})^{30} \times 27^3$

$\equiv 1 \times 27^3 \mod 100$

$= 83$

Th. if $a \equiv b \mod p$ and $a \equiv b \mod q$ } p, q are distinct primes

then $a \equiv b \mod pq$

Proof

$a \equiv b \mod p \Rightarrow p \mid (a-b)$ or $a - b = px$

$a \equiv b \bmod p \Rightarrow p \mid (a-b)$ or $a-b = px$

$a \equiv b \bmod q \Rightarrow q \mid (a-b)$ or $a-b = qy$

So,

$px = qy \Rightarrow p \mid qy$ but $p \nmid q$ so $p \mid y$

$\Rightarrow y = \alpha p \quad \alpha \in \mathbb{Z}$

$\therefore a-b = qy = \alpha pq$ for some $\alpha \geq 1$

or $pq \mid (a-b) \Rightarrow a \equiv b \bmod pq$

Public Key Cryptosystem (Framework)

cancel each other

P_A S_A — A ——— B — P_B S_B

P_B public key (everyone knows)

S_B secure key (do not share)

C

① Secure messaging

A sends B the cyphertext $C = P_B(M)$

B reads the message $M = S_B(C)$

② Authentication توثيق

A sends B the cyphertext $C = S_A(P_B(M))$

B reads the message $M = S_B(P_A(C))$

RSA

1. Pick two large primes p, q

2. Let $n = p \times q$

3. Pick public key $e \ni \gcd(e, (p-1)\times(q-1)) = 1$

4. Compute secure key $d \ni de \equiv 1 \bmod (p-1)\cdot(q-1)$

M = original message C = cipher text

then,

$$C = M^e \bmod n \quad \text{encryption}$$

$$M = C^d \bmod n \quad \text{decryption}$$

Aqil Azmi at 3/23/2021 9:59 AM

Ex Let $p = 43$, $q = 59$

$n = p \times q = 43 \times 59 = 2537$

Pick $e = 13$, make sure $\gcd(13, \underbrace{42\times58}_{=2436}) = 1$

Compute $d \ni 13d \equiv 1 \bmod 2436$

Using Euclidean we get $d = 937$

Assume M = "ST|OP" (letter → numeric A=00, B=01, ...)

M_1 = 1819, M_2 = 1415

$C_1 = M_1^e \bmod n = 1819^{13} \bmod 2537 = 2081$

$C_2 = M_2^e \bmod n = 1415^{13} \bmod 2537 = 2182$

Recovering message,

$M_1 = C_1^d \bmod n = 2081^{937} \bmod 2537 = 1819$

Recovering message,

$M_1 = C_1^d \bmod n = 2081^{937} \bmod 2537 = 1819$

$M_2 = C_2^d \bmod n = 2182^{937} \bmod 2537 = 1415$

$$\sum_{k=1}^{n}\sum_{j=k+1}^{m}(j-k) = \sum_{k=1}^{n}\left[\sum_{j=k+1}^{m} j\right] - \sum_{k=1}^{n}\left[\sum_{j=k+1}^{m} k\right]$$

$$= k\cdot(m-(k+1)+1)$$

$$= k\cdot(m-k)$$

$$= \sum_{j=1}^{m} j - \sum_{j=1}^{k} j$$

$$= \frac{1}{2}m(m+1) - \frac{1}{2}k(k+1)$$

$$= \frac{1}{2}\left[\sum_{k=1}^{n}(m^2+m-k^2-k)\right]$$

$$= \frac{1}{2}\left[n(m^2+m) - \frac{n(n+1)(2n+1)}{6} - \frac{n(n+1)}{2}\right]$$

$$= \sum_{k=1}^{n} k(m-k) = m\sum_{k=1}^{n} k - \sum_{k=1}^{n} k^2$$

$$= m\,\frac{n(n+1)}{2} - \frac{n(n+1)(2n+1)}{6}$$

$$= \frac{n}{2}\left[m^2+m - \frac{(n+1)(2n+1)}{6} - \frac{n+1}{2} - \frac{m(n+1)}{2} + \frac{(n+1)(2n+1)}{6}\right]$$

$$= \frac{n}{2}\left[m^2+m - \frac{n+1}{2} - \frac{m(n+1)}{2}\right]$$

Q2 Show $\overline{(A-B)\cup B} = \bar{A}\cap\bar{B}$

⇓

① Show each element $x \in \overline{(A-B)\cup B}$ is also in $\bar{A}\cap\bar{B}$

$$\overline{(A-B)\cup B} = \{x \mid x \notin (A-B)\cup B\}$$
$$= \{x \mid \neg(x \in (A-B)\cup B)\}$$
$$= \{x \mid \neg(x \in (A-B) \vee x \in B)\}$$
$$= \{x \mid \neg((x \in A \wedge x \notin B) \vee x \in B)\}$$
$$= \{x \mid \neg(x \in B \vee (x \in A \wedge x \notin B))\}$$
$$= \{x \mid \neg((x \in B \vee x \in A) \wedge \underbrace{(x \in B \vee x \notin B)}_{T})\}$$
$$= \{x \mid \neg(x \in B \vee x \in A)\}$$
$$= \{x \mid x \notin B \wedge x \notin A\}$$
$$= \{x \mid x \in \bar{B} \wedge x \in \bar{A}\}$$
$$= \bar{A}\cap\bar{B}$$

Set $P = Q$ ① $P \subseteq Q$ ② $Q \subseteq P$

Q4 Sequence $a_{10} = -10$, $a_{11} = -12$, $a_{12} = -14$, ...

$d = -2$

Sum $\sum_{k=100}^{150} a_k$

Formula $a_k = a_1 + d(k-1)$

$a_{11} = -12 = a_1 - 2 \times 10 \Rightarrow a_1 = -12 + 20 = 8$

$a_k = 8 - 2(k-1) = 10 - 2k$

$$\sum_{k=100}^{150} (10 - 2k) = \sum_{k=100}^{150} 10 - 2\sum_{k=100}^{150} k$$

Induction: $\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$

Base case $(n=1)$

LHS $= \frac{1}{1 \times 2}$

RHS $= \frac{1}{2}$

} True

Inductive case

Assume it is True for n.

$$\text{LHS} = \sum_{k=1}^{n+1} \frac{1}{k(k+1)} = \left(\sum_{k=1}^{n} \frac{1}{k(k+1)}\right) + \frac{1}{(n+1)(n+2)}$$

$= \frac{n}{n+1}$ by induction hypothesis

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

$$= \frac{1}{n+1}\left[n + \frac{1}{n+2} \right]$$

$$= \frac{1}{n+1} \times \frac{n^2+2n+1}{n+2} = (n+1)^2$$

$$= \frac{n+1}{n+2} = \text{RHS}$$

$$* \sum_{k=1}^{n} \left(\sum_{m=k}^{n} mk \right) = k \cdot \left(\sum_{m=k}^{n} m \right) = \frac{1}{2}\left[n(n+1) - k(k-1) \right]$$

$$= \frac{1}{2}\left[n^2 + n - k^2 + k \right]$$

$$= \frac{1}{2}\left[n^2 k + nk - k^3 + k^2 \right]$$

$$= \frac{1}{2} \sum_{k=1}^{n} \left(n^2 k + nk - k^3 + k^2 \right)$$

$$= \frac{1}{2}\left[(n^2+n) \cdot \sum_{k=1}^{n} k - \sum_{k=1}^{n} k^3 + \sum_{k=1}^{n} k^2 \right]$$

$$= \frac{1}{2}\left[(n^2+n) \cdot \frac{n(n+1)}{2} - \frac{n^2(n+1)^2}{4} + \frac{n(n+1)(2n+1)}{6} \right]$$

$$= \frac{n(n+1)}{2}\left[\frac{n(n+1)}{2} - \frac{n(n+1)}{4} + \frac{2n+1}{6} \right]$$

$$= \frac{n(n+1)}{}\left[n(n+1) + 2n+1 \right]$$

$$= \frac{n(n+1)}{4}\left[\, n(n+1) + \frac{2n+1}{3} \,\right]$$

$$= \frac{n(n+1)}{12}\left[\, 3n^2 + 5n + 1 \,\right]$$

$$* \sum_{i=1}^{n} \left(\sum_{j=1}^{m} n^i \right) = m \times n^i = m \sum_{i=1}^{n} n^i = m\left(\frac{n^{n+1} - n}{n-1}\right)$$

$$= mn\left(\frac{n^n - 1}{n-1}\right)$$

Combinatorics

Basic counting principles

Sum rule

Do task T_1 or T_2 (not both)

$\#ways = |T_1| + |T_2|$

$|T_1|$: # ways to do task T_1

Product rule

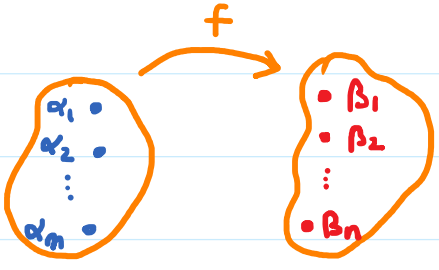
Do tasks T_1 and T_2

$\#ways = |T_1| \times |T_2|$

Ex

* Pick one item only from either box A or box B. # choices = $n + m$ (sum rule)
* Pick one item only from each box. # choices = $n \times m$ (product rule)

Ex How many functions are there from a set with m elements to a set with n elements.



$|A| = m$ $|B| = n$

Each $\alpha \in A$ has n choices

α_1 has n choices

α_2 " n "

α_m " n "

α_m " n "

functions $= n^m$ (product rule)

Ex A programming language allows a variable name of at most two characters case insensitive. How many variable names can we have if first character must be letter, and second character is alphanumeric.

Let V_1 = # variable names of length = 1

V_2 = # " " " length = 2

V = total # variable names $= V_1 + V_2$

$V_1 = 26$

$V_2 = 26 \times 36$

letter | letter or digit

A-Z | A-Z, 0-9

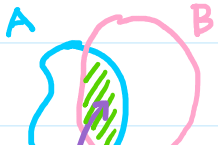
$V = 26 + 26 \times 36 = 962$

Aqil Azmi at 3/25/2021 10:03 AM

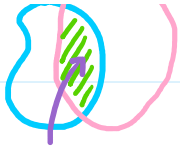
Principle of inclusion-exclusion

Overcounting ⇒ remove these elements

Undercounting ⇒ add " "



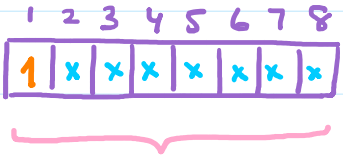
$|A \cup B| = |A| + |B| - |A \cap B|$



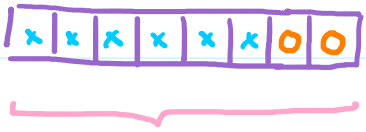
Counted twice

$$|A \cup B| = |A| + |B| - |A \cap B|$$

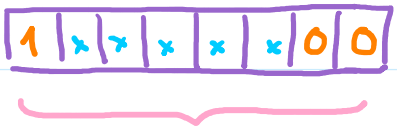
Ex How many bit strings of length 8 that either starts w/ 1 bit or ends w/ 00



patterns = $2^7 = 128$



patterns = $2^6 = 64$



this pattern was counted twice

patterns = $2^5 = 32$

bit strings = $128 + 64 - 32 = 160$

Pigeonhole Principle

Th if $k+1$ or more objects are placed into k boxes then there is at least one box with two or more objects.

Proof

Suppose each box has at most one object $\Rightarrow$ total # objects is at most k.

A contradiction since we have $k+1$ objects.

Ex Room with 13 people ⇒ Two or more must be born in same month.

Th Generalized Pigeonhole

if N objects are placed into k boxes, then there is at least one box containing at least $\lceil N/k \rceil$ objects.

Proof

For any $x \in \mathbb{R}$ then $x-1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x+1$

Suppose none of the boxes contains more than $\lceil N/k \rceil - 1$ objects.

Then, total # objects $\leq k \cdot (\lceil N/k \rceil - 1)$

$< k \cdot (((N/k) + 1) - 1) = N$

This contradicts as we have exactly N objects.

Ex Suppose we have 10 black, 10 brown, 10 white and 10 red socks. All mixed up.

How many to pick so to guarantee two socks of same color?

= smallest N satisfying $\lceil N/4 \rceil = 2$

(4 = # colors)

⇒ $N = 5$

To guarantee 2 black socks ⇒ pick 32 socks

Ex Given set of numbers: $1, 2, 3, \ldots, 25$. Pick any 14.
Show there is at least one pair that sums 26.

1	2	3	...	11	12	13
25	24	23	...	15	14	have 12 pairs
26	26	26		26	26	that sum 26

Pick 14. Worst scenario we pick $1, 2, \ldots, 13$. The 14th will be one of $14, 15, \ldots, 25$ and it will pair with one of the numbers to sum 26.

Permutation & Combination

Def. Permutation of a set of distinct objects is an ordered arrangement of these objects.
(order matter)

Th # of r-permutation of a set with n distinct elements is

$$P(n,r) = n \cdot (n-1) \cdot (n-2) \cdots (n-r+1) = \frac{n!}{(n-r)!}$$

Def. An r-combination of elements of a set is an unordered selection of r elements from set
(order not matter)

Th # r-combination of a set with n distinct elements and r an integer $(0 \le r \le n)$ is

$$C(n,r) = \binom{n}{r} = \frac{n!}{r! \cdot (n-r)!}$$

Ex Suppose we have 3 students. How many way to give 2 prizes. First = watch, second = pen.

ways = $P(3,2) = 6$

Ex Given 3 colored balls (red, blue, black). Pick 2 balls.

ways = $\binom{3}{2} = 3$

Ex Count # bit strings of length = 10 that has exactly 3 zeros.

$= \binom{10}{3}$ order does not matter as we are picking 3 zeros (ie. 3 identical items).

Ex Count # bit strings of length 10 that has at least 3 zeros.

$$= \binom{10}{3} + \binom{10}{4} + \binom{10}{5} + \cdots + \binom{10}{10} = \sum_{k=3}^{10} \binom{10}{k}$$

Ex. How many ways to arrange 10 books = $10!$

Ex Suppose we have 4 book in Arabic (A)
3 " " math (M)
3 " " CS (C)

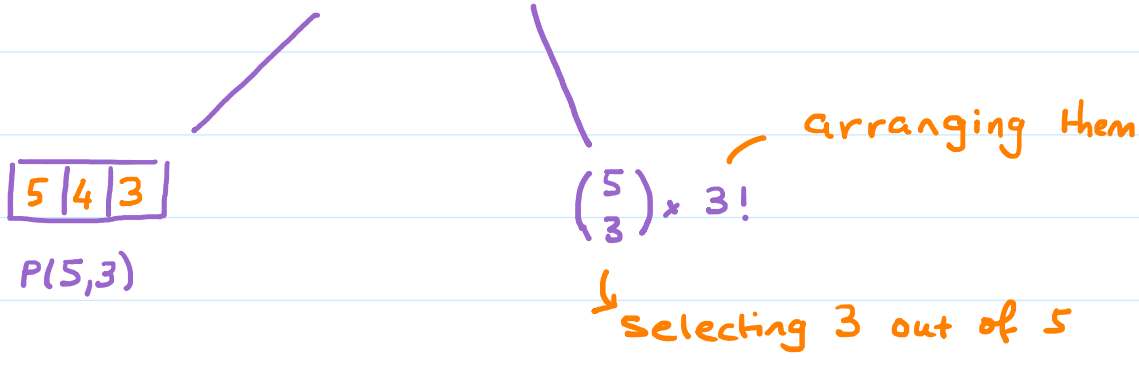
How many ways to arrange such that all book of a subject are together.

$= 3! \times 4! \times 3! \times 3!$

- $3!$: # ways to arrange by subject (AMC, ACM, ⋮)
- $4!$: # ways to arrange Arabic books
- $3!$: # ways to arrange math books
- $3!$: # ways to arrange CS books

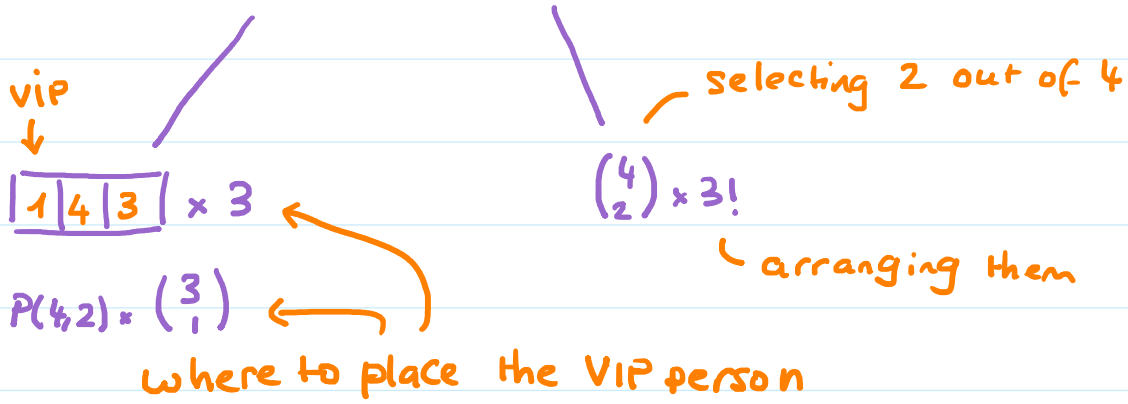
Aqil Azmi at 4/1/2021 10:05 AM

Ex. 5 people. How many ways to photograph them in groups of 3.



Ex. Suppose out of these 5 people one VIP person

must be in each picture.



Ex Computer passwords of length 6 ·· 8 characters. Character is either lowercase letter (a-z), or numeral. Each password must have at least one digit.

passwords = $P_6 + P_7 + P_8$ (# passwords of length = 6)

P_6 = # passwords of length 6 with one digit
+ # " " " " two digits
+ # " " " " three digits
⋮
+ # " " " " all digits

$$= \binom{6}{1} \times 10 \times 26^5 + \binom{6}{2} \times 10^2 \times 26^4 + \cdots + \binom{6}{6} \times 10^6$$

($\binom{6}{1}$: # places to put digit; 10: one digit; 10^2: 2 digit; 26^4: 4 letter)

$$= \sum_{k=1}^{6} \binom{6}{k} \times 10^k \times 26^{6-k} = 36^6 - 26^6$$

no restriction all letters

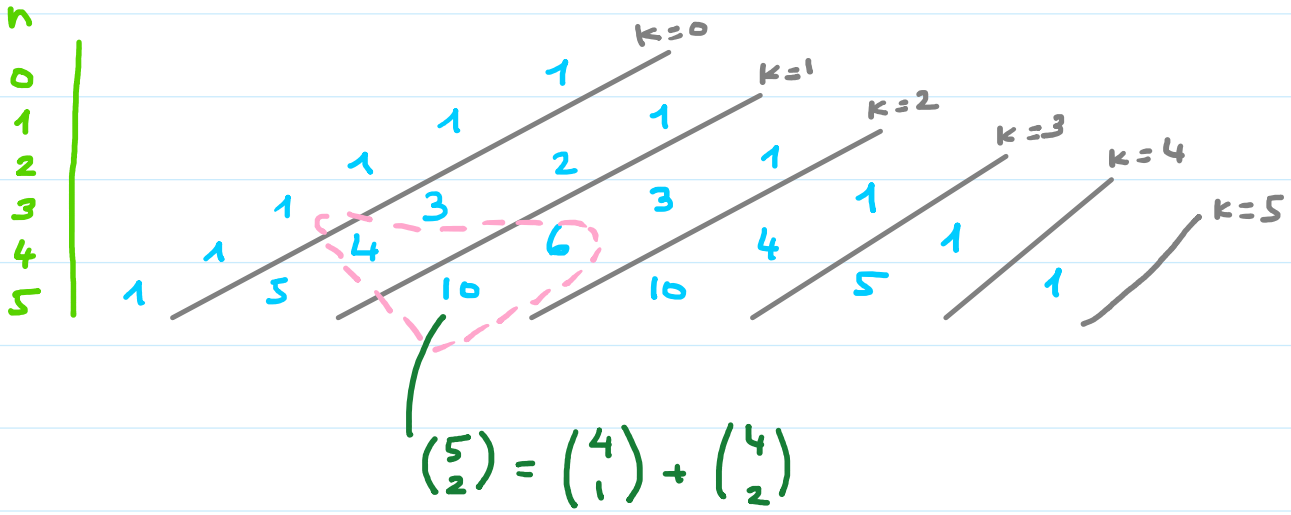
Similarly P_7 and P_8

$$\#\text{passwords} = \sum_{n=6}^{8} \sum_{k=1}^{n} \binom{n}{k} \times 10^{k} \times 26^{n-k}$$

Binomial Coefficient

Th Pascal's identity: let $n, k \in \mathbb{Z}^+$ with $n \geq k$, then

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$



$$\binom{5}{2} = \binom{4}{1} + \binom{4}{2}$$

Aqil Azmi at 4/6/2021 10:04 AM

Th Binomial Theorem

Let $x, y \in \mathbb{R}$ and $n \in \mathbb{Z}^+$ then

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \cdot y^{n-k} = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} \cdot y^k$$

$$= x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \cdots + y^n$$

Ex $(x+y)^2 = \sum_{k=0}^{2} \binom{2}{k} x^{2-k} \cdot y^k = x^2 + 2xy + y^2$

Ex $(x+y)^4 = \sum_{k=0}^{4} \binom{4}{k} x^{4-k} \cdot y^k = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$

Th. Let $n \in \mathbb{Z}^+$ then $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

Proof. In Binomial Th., let $x = y = 1$.

Th. Let $n \in \mathbb{Z}^+$ then $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$

Proof. In Binomial Th., let $x = 1$, $y = -1$.

Th Vandermonde's Identity.

Let $n, m, r \in \mathbb{N}$ with $r \leq \min(n, m)$. Then

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k} \cdot \binom{n}{k}$$

Corollary $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$

Proof. Use Vandermonde with $m = r = n$. And $\binom{n}{n-k} = \binom{n}{k}$.

Ex. Find coeff of x^{12} in $(3x - 5/x^2)^{30}$.

$$(3x - 5/x^2)^{30} = \sum_{k=0}^{30} \binom{30}{k} (3x)^k \cdot (-5/x^2)^{30-k}$$

$$= 3^k \cdot (-5)^{30-k} \cdot x^k \cdot (x^{-2})^{30-k}$$

$$= 3^k \cdot (-5)^{30-k} \cdot x^{3k-60}$$

Want $3k - 60 = 12 \Rightarrow k = 24$

$\therefore$ coeff of x^{12} is $\binom{30}{24} \cdot 3^{24} \cdot (-5)^6$

Th Multinomial Theorem

If n is positive integer, then

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{n_1 + n_2 + \cdots + n_k = n} C(n; n_1, n_2, \ldots, n_k)\, x_1^{n_1} \cdot x_2^{n_2} \cdots x_k^{n_k}$$

$C(n; n_1, n_2, \ldots, n_k)$: multinomial coeff

$$= \frac{n!}{n_1! \cdot n_2! \cdots n_k!}$$

Short

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{n_1 + n_2 + \cdots + n_k = n} \frac{n!}{n_1! \cdot n_2! \cdots n_k!} \prod_{i=1}^{k} x_i^{n_i}$$

Ex Expand $(x + y + z)^2 = \sum_{a+b+c=2} \frac{2!}{a! \cdot b! \cdot c!} x^a y^b z^c$

a	b	c	
2	0	0	$= x^2$
1	1	0	$= 2xy$
0	2	0	$= y^2$
1	0	1	$= 2xz$
0	0	2	$= z^2$
0	1	1	$= 2yz$

$$\therefore (x+y+z)^2 = x^2 + 2xy + y^2 + 2xz + z^2 + 2yz$$

Aqil Azmi at 4/8/2021 10:04 AM

Generalized Permutation and Combination

- r-permutation: select r objects out of n such that order matters.

w/o repetition: $P(n,r) = \frac{n!}{(n-r)!}$

w/ repetition: n^r

Ex. How many 5 letter words in English. $\boxed{26|26|26|26|26} = 26^5$

- r-combination: pick any r objects out of n such that order does not matter.

w/o rep.: $\binom{n}{r} = \frac{n!}{r! \cdot (n-r)!}$

w/ rep.: $\binom{n+r-1}{r}$ $\exists\ r \geq 0$

Ex. 10 apples, 10 oranges, 10 banana.

Pick 2 different fruits $= \binom{3}{2} = 3$

Pick any 2 fruits $= \binom{3+2-1}{2} = \binom{4}{2} = 6$

Ex. Consider eq. $x+y+z = 11$. How many integer solutions do we have for this eq. if $x, y, z \geq 0$.

Think of it as having 3 different kind of fruits. Pick 11.

$n = 3$, $r = 11$.

Solutions $= \binom{3+11-1}{11} = \binom{13}{11} = 78$

Ex. Suppose $x+y+z = 11$. How many solutions if $x \geq 1$, $y \geq 2$, $z \geq 4$.

Since $x \geq 1$, $y \geq 2$ and $z \geq 4$. The min of $x+y+z = 1+2+4 = 7$.

So they already selected 7 fruits for you. What you have choice is to pick the remaining 4 $(= 11-7)$ fruits.

So # Solutions of eq. $x+y+z = 4$ $\ni$ $x, y, z \geq 0$.

$= \binom{3+4-1}{4} = \binom{6}{4} = 15$.

Check

apple	orange	banana
1	2	8
1	3	7
1	4	6
1	5	5
1	6	4
2	2	7
2	3	6
2	4	5
2	5	4
3	2	6
3	3	5
3	4	4

3	3	5
3	4	4
4	2	5
4	3	4
5	2	4

Ex. Find # Solutions to $5 \leq x+y+z \leq 11$ $\quad x,y,z \geq 0$

$= \#$ Solution of $x+y+z=5$

$+ \#$ " " $x+y+z=6$

$\vdots$

$+ \#$ " " $x+y+z=11$

$$= \sum_{r=5}^{11} \binom{3+r-1}{r}$$

Permutations with indistinguishable objects

Ex How many different words can we make by re-arranging the letters of "SUCCESS".

$$\# \text{ distinct words} = \frac{7!}{2! \times 3!}$$

7! ~ # letters in "SUCCESS"

2! ~ # C's, 3! ~ # S's

Aqil Azmi at 4/11/2021 8:06 AM

Ex Consider letters: A, B, C, D, E.

1. # words of length = 5 (duplicates allowed) $= 5^5$
2. # words of length = 4 (duplicate letters allowed) $= 5^4$
3. # " " length = 5 (each letter once) $= 5!$

4. # " " length = 4 (" " ") = $P(5,4)$

5. # " " length = 3 (" " ") = $P(5,3)$ 5|4|3

6. # words of length = 5 (each letter once) and A, B together $= 4! \times 2!$

AB BA

7. # words of length = 5 (each letter once) and A, B not together $= 5! - 4! \times 2!$

8. # words of length = 5 (each letter once) and letters A, B, C are together $= 3! \times 3!$

ABC D E

ABC
ACB
⋮
CBA

Ex. Count # integers between 1 and 100 that are divisible by 6

divisible by 6 are: 6, 12, 18, 24, ...

$6K \leq 100 \qquad (K \geq 1)$

$\therefore K = \left\lfloor \frac{100}{6} \right\rfloor = 16$

Ex Count # integers between 1 and 100 that are divisible by 12 and 18.

$= \left\lfloor \frac{100}{\text{lcm}(12,18)} \right\rfloor = \left\lfloor \frac{100}{36} \right\rfloor = 2$ Check: 36, 72

Ex Count # integers between 1 and 100 that are

divisible by 12 or 18.

= # of those divisible by 12

+ # of those divisible by 18

− # of those common to 12 and 18

$$= \left\lfloor \frac{100}{12} \right\rfloor + \left\lfloor \frac{100}{18} \right\rfloor - \left\lfloor \frac{100}{\text{lcm}(12,18)} \right\rfloor = 11$$

Ex. Count # integers between 150 and 500 that are divisible by 12 or 18.

= Count # between 1 .. 500 − Count those 1 .. 149

$$= \left\lfloor \frac{500}{12} \right\rfloor + \left\lfloor \frac{500}{18} \right\rfloor - \left\lfloor \frac{500}{\text{lcm}(12,18)} \right\rfloor$$

$$- \left(\left\lfloor \frac{149}{12} \right\rfloor + \left\lfloor \frac{149}{18} \right\rfloor - \left\lfloor \frac{149}{\text{lcm}(12,18)} \right\rfloor \right)$$

آخر الدعوى - والحمد لله رب العالمين