# CSC 281: Discrete Mathematics

Aqil M Azmi

# 1 Foundations: Logic, Sets and Functions

## 1.1 Logic

**Def. 1 Proposition***: is a statement that is either true or false, but not both.*

- Examples:

  1. Riyadh is the capitol of Saudi Arabia.
  2. $1 + 5 = 4$.
  3. $x + y = y + x$ for $\forall x, y \in \mathbb{R}$.
  4. How are you?
  5. What are you doing.
  6. $x + 3 = 2$.

  The first three are propositions, while 4 and 5 are not statements. The last one is not a proposition (since can't determine the truth as it depends on the value of $x$).

- Letters are used to denote propositions $p, q, r, s$. $T$ =true, $F$ =false.
- Compound proposition: form new proposition out of existing ones using logical operators.
- Truth table: display relationship between truth values of propositions.
- Negation: $\neg p$ (not $p$).
- Connectives: logical operators that form new proposition from 2+ existing propositions.
- AND $(p \wedge q)$; OR $(p \vee q)$; XOR $(p \oplus q)$; Implication $(p \rightarrow q)$, here $p$ is called hypothesis and $q$ is the conclusion or the consequence.

| $p$ | $q$ | $p \oplus q$ |
|---|---|---|
| F | F | F |
| F | T | T |
| T | F | T |
| T | T | F |

| $p$ | $q$ | $p \to q$ |
|---|---|---|
| F | F | T |
| F | T | T |
| T | F | F |
| T | T | T |

- Example:
  `if 2+2=4 then x := x+1;`
  if `x=5` before this statement then it will be 6 after the execution of the statement.
- Shorthand for $(p \vee q) \wedge (\neg r)$ is $(p \vee q) \wedge \neg r$.
- The converse of $p \to q$ is the proposition $q \to p$.
- The contrapositive of $p \to q$ is the proposition $\neg q \to \neg p$.
- Biconditional $p \leftrightarrow q \equiv p \to q \wedge q \to p$. Note that it is $T$ iff $p = q$.
- Example:
  Let $p =$ 'I live in Riyadh,' $q =$ 'I am in Saudi Arabia.' Here $p \to q$ but the converse is false, while the contrapositive is true.
- Example:
  Let $p =$ 'I am rich,' $q =$ 'I can afford a Roles-Royce.' Here $p \to q$ and both the converse as well as the contrapositive are all true.
- Logic and bit operation. Bit = Binary Digit = 0 or 1. A Boolean variable is a variable that is either $T$ or $F$. Bitstring is a sequence of $\geq 0$ bits.

| $\vee$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 1 |

- Bitwise OR, bitwise AND and bitwise XOR.
- Construct a truth table for $(p \leftrightarrow q) \vee (\neg p \leftrightarrow q)$.

## 1.2 Propositional Equivalences

**Def. 2 Tautology**: *compound proposition which is always $T$ regardless of the truth values of the propositions that occur in it.*

**Def. 3 Contradiction**: *compound proposition which is always $F$.*

- Examples:
  Show using truth table
  $p \vee \neg p$ is a tautology.
  $p \wedge \neg p$ is a contradiction.
- Logically equivalent means always having the same truth values.

  **Def. 4** *Propositions $p$ and $q$ are called logically equivalent if $p \leftrightarrow q$ is a tautology.*

  *Notation: $p \Leftrightarrow q$ means $p$ and $q$ are logically equiv.*
- Show $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$ using truth table. This is known as DeMorgan's law.
- Extended DeMorgan's law:
  $\neg(p_1 \vee p_2 \vee \cdots \vee p_n) \Leftrightarrow \neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_n$.
  $\neg(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \Leftrightarrow \neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_n$.
- Example:
  Show $p \rightarrow q$ and $\neg p \vee q$ are logically equiv using truth table.
- Example:
  Show $p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$ are logically equiv using truth table.
- In general for $n$ propositions need truth table with $2^n$ rows.
- Logical equivalences:

| Equivalences | Name |
|---|---|
| $p \wedge T \Leftrightarrow p$<br>$p \vee F \Leftrightarrow p$ | identity |
| $p \vee T \Leftrightarrow T$<br>$p \wedge F \Leftrightarrow F$ | domination |
| $p \vee p \Leftrightarrow p$<br>$p \wedge p \Leftrightarrow p$ | idempotent |
| $\neg(\neg p) \Leftrightarrow p$ | double negation |
| $p \vee q \Leftrightarrow q \vee p$<br>$p \wedge q \Leftrightarrow q \wedge p$ | commutative |
| $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$<br>$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$ | associative |
| $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$<br>$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$ | distributive |
| $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$<br>$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$ | DeMorgan |
| $p \vee \neg p \Leftrightarrow T$<br>$p \wedge \neg p \Leftrightarrow F$<br>$(p \rightarrow q) \Leftrightarrow \neg p \vee q$ | useful logical equivalences |

- Example:
  Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equiv.

$$\begin{aligned}
\neg(p \vee (\neg p \wedge q)) &\Leftrightarrow \neg p \wedge \neg(\neg p \wedge q) \\
&\Leftrightarrow \neg p \wedge (p \vee \neg q) \\
&\Leftrightarrow (\neg p \wedge p) \vee (\neg p \wedge \neg q) \\
&\Leftrightarrow F \vee (\neg p \wedge \neg q) \\
&\Leftrightarrow \neg p \wedge \neg q
\end{aligned}$$

- Determine if $\neg(p \wedge (p \to q)) \to \neg q$ is tautology.

$$\begin{aligned}
\neg(p \wedge (p \to q)) \to \neg q &\Leftrightarrow (p \wedge (p \to q)) \vee \neg q \\
&\Leftrightarrow \neg q \vee (p \wedge (p \to q)) \\
&\Leftrightarrow (\neg q \vee p) \wedge (\neg q \vee (p \to q)) \\
&\Leftrightarrow (\neg q \vee p) \wedge (\neg q \vee \neg p \vee q) \\
&\Leftrightarrow (\neg q \vee p) \wedge T \\
&\Leftrightarrow q \to p \\
&\not\Leftrightarrow T
\end{aligned}$$

## 1.3 Predicates and Quantifiers

- The statement $x > 5$ is neither true or false (since we don't know the value of variable $x$). How can we make *propositions* out of such statement. Now $x > 5$ has two parts

$$\underbrace{x}_{\text{subject of statement}} \qquad \underbrace{> 5}_{\text{predicate}}$$

  where predicate refers to a property the subject of statement can have.

- Lets denote the statement $x > 5$ by $P(x)$ where $P$ is the predicate "$> 5$".

- Statement $P(x)$ has the value of the propositional function $P$ at $x$, i.e once $x$ has a value assigned then $P(x)$ has a truth value.

- Example:
  Let $P(x)$ denote the statement "$x > 5$," then the truth value of $P(4)$ is $F$ (since $4 > 5$ is $F$), while $P(9)$ is $T$.

- Similarly, for statement $x = y + z - 2$ can be denoted by $Q(x, y, z)$. $\ni x, y, z$ are variables and $Q$ is predicate. Here, the truth value of $Q(3, 2, 0)$ is $F$, while $Q(7, 8, 1)$ is $T$.

- In general, a statement with $n$ variables $x_1, x_2, \ldots, x_n$ can be denoted by $P(x_1, x_2, \ldots, x_n)$ where $P$ is predicate.

  A statement of this form is the value of the propositional function $P$ at $x_1, x_2, \ldots, x_n$.

- Another way to change propositional functions into propositions, called quantification.

- Two types:
  - universal quantification.
  - existential quantification.

  **Def. 5** *The universal quantification of $P(x)$ is the propositional "$P(x)$ is true for all values of $x$ in a particular domain (called universe of discourse)."*

- $\underbrace{\forall x P(x)}_{\text{for every } x \ P(x)}$ denotes universal quantification of $P(x)$.

- Example:
  Let $P(x)$ be the statement "$x + 1 > x$," what is the truth value of quantification $\forall x P(x)$ where universe of discourse is $\mathbb{R}$.
  Since $P(x)$ is true for all $x \in \mathbb{R}$ then $\forall x P(x)$ is true.

- Example:
  Let $Q(x)$ be the statement "$x < 2$," what is $\forall x Q(x)$ where universe of discourse is $\mathbb{R}$.
  Since $Q(x)$ is not true for all $x \in \mathbb{R}$ (e.g $x = 2$) so $\forall x Q(x)$ is false.

- Let the universe of discourse be $\{x_i \mid 1 \leq i \leq n\}$, then the universal quantification $\forall x P(x)$ is same as the $P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n)$, which is true if all $P(x_1), P(x_2), \ldots, P(x_n)$ are all true.

- Example:
  What is $\forall x P(x)$ if $P(x)$ be the statement "$x^2 < 11$" and universe of discourse is $\{1, 2, 3, 4\}$.
  Since $\forall x P(x)$ is same as $\bigwedge_{i=1}^{4} P(i)$ but $P(4)$ is $F$, thus $\forall x P(x)$ is false.

  **Def. 6** *The existential quantification of $P(x)$ is the proposition "There $\exists$ an element $x$ in the universe of discourse $\ni$ $P(x)$ is true."*

- $\underbrace{\exists x P(x)}_{\text{for some } x \ P(x)}$ denotes universal existential of $P(x)$.

- Example:
  Let $P(x)$ be the statement "$x \geq 3$." What is $\exists x P(x)$ where universe of discourse is $\mathbb{R}$.
  Since "$x \geq 3$" is true for instance when $x = 3$ then $\exists x P(x)$ is true.

- Example:
  Let $P(x)$ be the statement "$x = x - 1$," what is $\exists x P(x)$ where the universe of discourse is $\mathbb{R}$. Since $P(x)$ is false for all $x \in \mathbb{R} \Rightarrow \exists x P(x)$ is false.

- In general, let the universe of discourse be $\{x_1, x_2, \ldots, x_n\}$ then the existential quantification $\exists x P(x)$ is as the $P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n)$, which is true iff at least one of $P(x_1), P(x_2), \ldots, P(x_n)$ is true.

- Example:
  What is $\exists x P(x)$ if $P(x)$ is the statement "$x^2 < 11$" and universe of discourse is $\{1, 2, 3, 4\}$.
  Since $\exists x P(x)$ is the same as $\bigvee_{i=1}^{4} P(i)$ and $P(1)$ is the statement $1 < 11$ is true, therefore $\exists x P(x)$ is true.

- Express the statement "Everyone has a father."
  Let $F(x, y)$ be the statement "$y$ is the father of $x$," then the solution is:
  $\forall x\ \exists y\ F(x, y)$, where the universe of discourse is all human being.

- Express "Everyone has a *single* father."
  Let $F(x, y)$ as before, then the solution is:
  $\forall x\ \exists y\ \forall z\ (F(x, y) \wedge ((z \neq y) \rightarrow \neg F(x, z)))$, where the universe of discourse is all human being.
  I.e for every person $x$, there is another person $y, \ni y$ is the father of $x$ and if $z$ is a person other than $y$ then $z$ is not the father of $x$.

- Express "Everyone has a father and a mother."
  Let $F(x, y)$ as before, and let $M(x, y)$ be the statement "$y$ is the mother of $x$," then the solution is:
  $\forall x\ \exists y\ \exists z\ F(x, y) \wedge M(x, z)$, where the universe of discourse is all human being.
  Another solution is, let $F(x)$ and $M(x)$ be the statements "$x$ has a father (mother), respectively," then we can solve it as:
  $\forall x\ F(x) \wedge M(x)$.

- Express "Everyone is either a male or a female."
  Let $M(x)$ be the statement "$x$ is male," and $F(x)$ be the statement "$x$ is female," then the solution is:
  $\forall x\ M(x) \oplus F(x)$.

- Express "If someone is a male and is a parent then he is some ones father."
  Let $M(x)$ be the statement "$x$ is male,"
  $P(x)$ be the statement "$x$ is parent,"

  $F(x, y)$ be the statement "$x$ is father of $y$," then solution is:

  $\forall x\ ((M(x) \wedge P(x)) \rightarrow \exists y\ F(x, y))$.

- Prolog (PROgramming in LOGic) is a programming language used in AI to solve logic related problems.

- A variable is either bound or free.

- Bound variable:

  - When a quantifier is used on a variable.
  - When we assign a value to a variable.

- Free variable: not bound by either the quantifier nor assigned a value.

- All variables which occur in propositional function must be bound so to turn it into a proposition.

- Order of quantifiers is important unless all are $\forall$ or $\exists$, i.e
  $\forall x\ \forall y \equiv \forall y\ \forall x$
  $\exists x\ \exists y \equiv \exists y\ \exists x$.

- Example:
  Let $Q(x, y)$ denote "$x+y = 0$" what is the truth value of the quantification:

  - $\exists y\ \forall x\ Q(x, y)$ means "there is a real number $y \ni \ \forall$ real number $x, Q(x, y)$ is true." This quantification is false. It follows the reasoning: "now if we pick any $y$, there is only one $x$ for which $x + y = 0$. Since there is no single $y \ni \ x + y = 0 \ \Rightarrow$ false.
  - $\forall x\ \exists y\ Q(x, y)$ means "for every $x$ exists a real number $y \ni \ Q(x, y)$ is true." This quantification is true. The reason behind is: "now for any $x$ there is a real number $y \ni \ x + y = 0$, namely $y = -x \ \Rightarrow$ sentence is true.

  Hence $\exists y\ \forall x\ Q(x, y) \not\Longleftrightarrow \forall x\ \exists y\ Q(x, y)$.

- Example:
  Let $Q(x, y)$ denote "$x + y = z$." Again here we get
  $\forall x\ \forall y\ \exists z\ Q(x, y, z) \not\Longleftrightarrow \exists z\ \forall x\ \forall y\ Q(x, y, z)$,
  where the former is true and latter is false.

- What about the negation of a quantified expressions. Consider the statement: "Every student in the class knows Arabic." Clearly this statement is a universal quantification, $\forall x P(x)$ is $\ni P(x)$ is "$x$ knows Arabic."
  The negation of this statement is "There is a student in this class who doesn't know Arabic," which can be expressed as $\exists x\ \neg P(x)$. Thus
  - $\neg\forall x\ P(x) \Leftrightarrow \exists x\ \neg P(x)$.
  - $\neg\exists x\ Q(x) \Leftrightarrow \forall x\ \neg Q(x)$

$$- \neg\big(\forall x P(x)\big) \Leftrightarrow \exists x \neg P(x)$$
$$- \neg\big(\exists x Q(x)\big) \Leftrightarrow \forall x \neg Q(x)$$

## 1.4 Sets

- Sets is a collection of objects.
- Sets are used to group objects together. Often (though not necessary) objects in a set have similar properties.

  **Def. 7** *Objects in a set are called members or elements of the set. A set is said to contain elements.*

- Example:
  The set of prime numbers $< 20$ are expressed as: $\{2, 3, 5, 7, 11, 13, 17, 19\}$.
  We may also express it as: $\{x \mid x \text{ is prime integer } < 20\}$.

  **Def. 8** *Two sets are equal iff they have the same elements, e.g* $\{2, 3, 9\}$ *and* $\{3, 2, 9\}$.

- Empty set or null set, denoted by $\emptyset$, also denoted by $\{\}$.

  **Def. 9** *Set A is subset of set B if every element of A is also in B. Denoted* $A \subseteq B$. *Using quantification:*
  $\forall a\ (a \in A \rightarrow a \in B)$.

- Null set is a subset of every set, i.e $\emptyset \in S$.

  **Def. 10** *The cardinality of set S is the number of distinct elements in S. It is denoted by* $|S|$.

- $|\emptyset| = 0$.

  **Def. 11** *A set is said to be infinite if it is not finite.*

- Example:
  The set of positive integers is infinite.

  **Def. 12** *The power set of the set S is the set of all subsets of the set S. Denoted by* $P(S)$.

- Example:
  The power set of $\{a, b, c\}$ is $\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$.
- $|P(S)| = 2^{|S|}$.

**Def. 13** *The ordered n-tuple* $(a_1, a_2, \ldots, a_n)$ *is the ordered collection that has* $a_1$ *as its first element,* $a_2$ *as its second element,* $\ldots, a_n$ *is its final element.*

**Def. 14** *The cartesian product of sets* $A$ *and* $B$*, denoted* $A \times B$*, is the set of all ordered pairs* $(a, b) \ni a \in A$ *and* $b \in B$*. Thats* $A \times B = \{(a, b) \,|\, a \in A \wedge b \in B\}$*.*

- Example:
  Let $A = \{1, 2\}$ and $B = \{a, b, c\}$, then $A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$
- Note that $A \times B \neq B \times A$ unless $A = B$ or $A = \emptyset$ or $B = \emptyset$. The latter $A \times \emptyset = \emptyset$.
- In general:
  $A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \,|\, a_i \in A_i,\ 1 \leq i \leq n\}$
- There are two problems with the theory of sets which is known as the naive set theory: (1) leads to paradox; (2) not very practical for many real life situations.

  1. The paradoxes of set theory
     The naive set theory ultimately leads to logical inconsistencies (known as paradoxes) $\Rightarrow$
     - Either abandon set theory.
     - Patch the set theory which would eliminate the paradoxes (recall that originally, set is a collection of objects).

     Following is two examples on paradoxes, including Russell's.

     (a) *The barber's paradox*
     In a small city, a barber said: "I shave every man (except those men who shave themselves."
     Does the barber shave himself?
     NO: He's not an exception
     $\Rightarrow$ he shaves himself (contradiction).
     Yes: He's an exception
     $\Rightarrow$ he does not shave himself (a contradiction).
     $\Rightarrow$ Barber is not a man!

     (b) *Russell's paradox (1902)*
     Before we proceed, an example of set of sets. Power set is one such example, another is $\{\{a, b, c\}, \{1, 2, 3\}\}$.
     Let $S$ be the set of all non-empty sets, so $\emptyset \notin S$. Define Russell's set $X$ as: $X$ contains every set (except sets which contain themselves).

Does $X$ contain itself?
NO: not an exception
$\Rightarrow$ $X$ does contain $X$ (contradiction).
Yes: is an exception
$\Rightarrow$ $X$ does not contain $X$ (contradiction).
$\Rightarrow$ $X$ is not a set (called class).

2. Fuzzy sets
Consider, $A = \{x \mid x \text{ is a tall person in this class}\}$. Say we have these people w/height: Ali, 1.99m; Ahmad, 1.92m; Ayman, 1.76m; Aziz, 1.75m; Sammer, 1.72m; Aamir, 1.52m and Zaid 1.43m. Which of these should be in the group. Another example is the list of speeding cars.

The theory of fuzzy sets deals with a subset $A$ of the universe of discourse $X$, where the transition between full membership and no membership is gradual rather than abrupt. The 'fuzzy sets' has no well-defined boundaries where the universe of discourse $X$ covers a definite range of objects. Traditionally, the grade of membership 1 is assigned to those objects that fully and completely belongs to $A$ while 0 is assigned to objects that do not belong to $A$ at all. The more an object $x$ belongs to $A$, the closer to 1 is its grade of membership $\chi_A(x)$. The grade of membership is $0 \leq \chi_A(x) \leq 1$.
Let $X = \{x\}$, then a fuzzy set $A$ in $X$ is a set of ordered pairs

$$A = \{(x, \chi_A(x))\},\ x \in A.$$

Fuzzy sets was introduced by Lutfi Zadeh in 1965.

Another example. Let $A = \{x \mid x \text{ is a real number and } x \gg 1\}$. Here we define the membership function as

$$\chi_A(x) = \begin{cases} 0 & \text{if } x \leq 1 \\ \frac{x-1}{x} & \text{for } x > 1 \end{cases}$$

another possible membership function

$$\chi_A(x) = \begin{cases} 0 & \text{if } x \leq 1 \\ e^{-(x-1)} & \text{for } x > 1 \end{cases}$$

## 1.5 Set Operations

**Def. 15** *Let $A, B$ be sets, then the union of both sets is the set*

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

**Def. 16** *Let $A, B$ be sets, then the intersection of both sets is the set*

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

**Def. 17** *If $A \cap B = \emptyset$ then they are called disjoint sets.*

**Def. 18** *Let $A, B$ be sets, the difference of $A$ and $B$ is the set*

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

**Def. 19** *Let $U$ be the universal set. The complement of set $A$, denoted $\bar{A}$ is the set*

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

- Set identities:

| Set identity | Name |
|---|---|
| $A \cup \emptyset = A$<br>$A \cap U = A$ | identity |
| $A \cap \emptyset = \emptyset$<br>$A \cup U = U$ | domination |
| $A \cup A = A$<br>$A \cap A = A$ | idempotent |
| $\bar{\bar{A}} = A$ | double complement |
| $A \cup B = B \cup B$<br>$A \cap B = B \cap A$ | commutative |
| $(A \cup B) \cup C = A \cup (B \cup C)$<br>$(A \cap B) \cap C = A \cap (B \cap C)$ | associative |
| $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$<br>$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ | distributive |
| $\overline{A \cup B} = \bar{A} \cap \bar{B}$<br>$\overline{A \cap B} = \bar{A} \cup \bar{B}$ | DeMorgan |

- Example:
  Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$.

$$\begin{aligned} \text{Suppose } x \in \overline{A \cap B} &\Rightarrow x \notin A \cap B \\ &\Rightarrow x \notin A \text{ or } x \notin B \\ &\Rightarrow x \in \bar{A} \text{ or } x \in \bar{B} \\ &\Rightarrow x \in \bar{A} \cup \bar{B} \\ &\Rightarrow \overline{A \cap B} \subseteq \bar{A} \cup \bar{B} \end{aligned}$$

$$\begin{aligned}
\text{Now suppose that } x \in \bar{A} \cup \bar{B} &\Rightarrow x \in \bar{A} \text{ or } x \in \bar{B} \\
&\Rightarrow x \notin A \text{ or } x \notin B \\
&\Rightarrow x \notin A \cap B \\
&\Rightarrow x \in \overline{A \cap B} \\
&\Rightarrow \bar{A} \cup \bar{B} \subseteq \overline{A \cap B}
\end{aligned}$$

combining the above two yields our desired result. Another proof which relies on logical equiv. is

$$\begin{aligned}
\overline{A \cap B} &= \{x \,|\, x \notin A \cap B\} \\
&= \{x \,|\, \neg(x \in A \cap B)\} \\
&= \{x \,|\, \neg(x \in A \wedge x \in B)\} \\
&= \{x \,|\, x \notin A \vee x \notin B\} \\
&= \{x \,|\, x \in \bar{A} \vee x \in \bar{B}\} \\
&= \{x \,|\, x \in \bar{A} \cup \bar{B}\}
\end{aligned}$$

### 1.5.1 Generalized Unions and Intersections

**Def. 20** *Union of a collection of sets is the set that contains those elements that are members of at least one set in the collection.*

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$$

**Def. 21** *Intersection of a collection of sets is the set that contains those elements which are common to all sets in the collection.*

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$$

- Example:

$$\begin{aligned}
A &= \{0, 2, 4, 6, 8\} \\
B &= \{0, 1, 3, 4\} \\
C &= \{0, 3, 6, 9\} \\
A \cup B \cup C &= \{0, 1, 2, 3, 4, 6, 8, 9\} \\
A \cap B \cap C &= \{0\}
\end{aligned}$$

**Def. 22** *Symmetric difference of sets $A, B$ is*

$$A \oplus B = \{x \,|\, (x \in A) \oplus (x \in B)\}$$

**Def. 23** *Multisets: collection of objects such that objects can occur more than once. Notation: $\{m_1 \cdot a_1, m_2 \cdot a_2, \ldots, m_n \cdot a_n\}$, where $a_i$ is the object and $m_i$ is # of times it occurs.*

- Example:
  $\{3 \cdot a, 2 \cdot b, 1 \cdot c\}$.
- Let $A = \{m_{i_A} \cdot x_i\}$ and similarly $B$, then

$$\begin{aligned} A \cup B &= \{m_i \cdot x_i \,|\, m_i = \max(m_{i_A}, m_{i_B})\} \\ A \cap B &= \{m_i \cdot x_i \,|\, m_i = \min(m_{i_A}, m_{i_B})\} \\ A - B &= \{m_i \cdot x_i \,|\, m_i = \max(m_{i_A} - m_{i_B}, 0)\} \end{aligned}$$

  For example, $A = \{1 \cdot a, 2 \cdot b\}, B = \{3 \cdot b, 2 \cdot c\}$ then $A \cup B = \{1 \cdot a, 3 \cdot b, 2 \cdot c\}, A \cap B = \{2 \cdot b\}$ and $A - B = \{1 \cdot a\}$.

## 1.6 Functions

**Def. 24** *Let $A, B$ be sets. Function from $A$ to $B$ is an assignment of <u>one</u> element of $B$ to each element of $A$.*

- $f\colon A \to B$, means $f$ maps $A$ to $B$. Here $A$ is domian of $f$, while $B$ is codomain of $f$.
- $f(a) = b$. Here $b$ is the image of $a$ under $f$, while $a$ is the preimage of $b$ under $f$.
- Range of $f$: set of all images of $A$. Thats $\{f(a) \,|\, \forall a \in A\}$.
- Example:
  Let $f\colon \mathbb{Z} \to \mathbb{Z}$ which assigns square of an integer to an integer, i.e $f(x) = x^2$. Range is $\{0, 1, 4, 9, \ldots\}$.

**Def. 25** *Let $f_1\colon A \to \mathbb{R}$ and similarly $f_2$. Then*

$$f_1 + f_2\colon A \to \mathbb{R}$$
$$f_1 f_2\colon A \to \mathbb{R}$$

*such that*

$$\begin{aligned} (f_1 + f_2)(x) &= f_1(x) + f_2(x) \\ (f_1 f_2)(x) &= f_1(x) f_2(x) \end{aligned}$$

**Def. 26** *Let $f: A \to B$, and let $S \subset A$ then the image of $S$ is*

$$f(S) = \{f(s) \mid s \in S\}$$

**Def. 27** *$f$ is <u>one-to-one</u> iff $f(x) = f(y) \Rightarrow x = y$ $\forall x, y$ in domain. I.e images of elements in its domain are all different.*

- Also, $f$ is one-to-one iff $f(x) \neq f(y)$ whenever $x \neq y$.
- A condition which guarantees $f$ to be 1–1 is if $f$ is strictly increasing (i.e $f(x) < f(y)$ if $x < y$) or strictly decreasing.

**Def. 28** *$f: A \to B$ is <u>onto</u> 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 $A$. Thats is all nodes of $B$ are used up.*

**Def. 29** *$f$ is one-to-one correspondence (bijective) if both 1–1 and onto.*

**Def. 30** *If $f: A \to B$ is 1–1 correspondence $\iff |A| = |B|$.*

- Let $f: A \to B$ then
  - $f$ is 1–1 if every node in $B$ has 0 or 1 incomming arrow.
  - $f$ is onto if every node in $B$ has $\geq 1$ incomming arrow(s).
  - $f$ is 1–1 and onto if every node in $B$ has exactly 1 incomming arrow.

**Def. 31** *Let $f: A \to B$ be 1–1 correspondence, then the inverse function of $f$ is $f^{-1}: B \to A$ $\ni a = f^{-1}(b)$ where $b = f(a)$.*

- If $f$ is only 1–1 then can't have $f^{-1}$ since $\exists$ $b \in B$ which is not an image of an $a \in A$. More clearly, since some nodes in $B$ has no incomming arrow.
- Similarly if $f$ is only onto then $\exists$ some $b \in B$ where we have $a_1, a_2 \in A$ $\ni$ $f(a_1) = f(a_2) = b$. More clearly, some nodes in $B$ has more than one incomming arrow.
- Therefore, if $f$ is only 1–1 or only onto then we say $f$ is not invertible.
- Example:
  Let $f: \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x + 1$. Here $f$ is 1–1 (since it is strictly increasing). So if $y = x + 1$ then $x = y - 1$, thats $f^{-1}(y) = y - 1$.
- Example:
  Let $f: \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$ is $f$ invertible?
  Since $f(-1) = f(1) = 1 \Rightarrow f$ is not 1–1 $\Rightarrow$ not invertible.

$a_{50} = 107$
$a_{51} = 110$ } $+3$
$a_{52} = 113$
$\vdots$

$a_n = a_1 + 3(n-1)$

find $a_{120}$ ?

$a_{52} = 113 = a_1 + 3 \times 51$

$a_1 = 113 - 3 \times 51 = -40$

$a_{120} = a_1 + 3 \times 119$

index

Aqil Azmi, PhD. at 9/20/2020 9:16 AM

find smallest index $K \ni a_K \geq 1000$ and $a_{K-1} < 1000$

$a_K = -40 + 3(K-1) \geq 1000$

$3K - 3 \geq 1040$

$3K \geq 1043$

$K = \left\lceil \frac{1043}{3} \right\rceil = 348$

$\leq$

$a_{348} = -40 + 3 \times 347 = 1001$

Consider sequence: 1, 7, 25, 79, 241, 727, ...

$\frac{25}{7} = 3.57$ $\frac{79}{25} = 3.16$ $\frac{241}{79} = 3.05$

$\frac{727}{241} = 3.02$ ratio $\to 3$

formula $a_n$ will have $3^n$

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| $3^n$ | 3 | 9 | 27 | 81 | 243 | 729 | ... |

$a_n = 3^n - 2$ $n \geq 1$ $a_7 = 3^7 - 2 = 2185$

Consider Sequence: 4, 5, 7, 11, 19, 35, 67, 131, ...

$\frac{5}{4} = 1.25$ $\frac{7}{5} = 1.4$ $\frac{11}{7} = 1.57$ $\frac{19}{11} = 1.727$

$\frac{35}{19} = 1.84, \ldots$ ratio $\to 2$

formula $a_n$ have $2^n$

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $2^n$ | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 |

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

Tuesday, September 22, 2020

# Summations

given sequence $a_1, a_2, a_3, \cdots$

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n$$

$n$ ← upper bound

$i = 1$ ← lower bound

$i$ ↑ index

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

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

Proof

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

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

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

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

$m \leq n$

$n + (n - m)$

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

$$= \underbrace{m + m + \cdots + m}_{n-m+1} + 1 + 2 + \cdots + ? \quad n-m$$

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

$$= \underbrace{m + (m+1) + \cdots + n}_{1+2+3+\cdots+(m-1)+} \underbrace{- 1 - 2 - 3 - \cdots - (m-1)}$$

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

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

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

Aqil Azmi, PhD. at 9/27/2020 8:57 AM

calculate $\sum_{\substack{K=1 \\ K \text{ odd}}}^{20} K = 1 + 3 + 5 + 7 + \cdots + 19$

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

n 2 2 2 $\left(\frac{n}{2}\right)^2$

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

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

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

## Double summations

$$\sum_{i=1}^{n} \sum_{j=1}^{m} c = cmn$$

$m \geq n$

$$\sum_{i=1}^{n} \underbrace{\sum_{j=i}^{m} c}$$

$$= \sum_{j=1}^{m} c - \sum_{j=1}^{i-1} c$$

$$= c \cdot m - c(i-1)$$

$$= \sum_{i=1}^{n} (cm - c(i-1))$$

$$= \sum_{i=1}^{n} cm - \sum_{i=1}^{n} c(i-1)$$

$$= cmn - c \boxed{\sum_{i=1}^{n} (i-1)}$$

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

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

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

$$= cn\left[m - \frac{n-1}{2}\right]$$

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

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

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

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

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

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

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

$$n(n+1)\left[ 2n+1 \right]$$

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

$$\prod_{i=1}^{n} C = \underbrace{C \times C \times \cdots \times C}_{n \text{ terms}} = C^n$$

$$\prod_{i=1}^{n} i = n!$$

Aqil Azmi at 9/29/2020 9:15 AM

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

$$m + m + m + \cdots + m$$

$$\#\text{terms} = n - m + 1$$

$$= m \times (n - m + 1)$$

$$1 + 2 + \cdots + (n-m)$$

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

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

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

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

Find the sum of $\sum_{\substack{i=1 \\ i \text{ odd}}}^{n} i = ?$

$= 1 + 3 + 5 + \cdots + \begin{cases} n & n \text{ odd} \\ n-1 & \text{if } n \text{ even} \end{cases}$

recall odd # generator $2K-1$

K must be $1, 2, 3, \ldots, ?$

$2K-1 \leq n \Rightarrow K = \left\lfloor \frac{n+1}{2} \right\rfloor$ → $K \leq \frac{n+1}{2}$

$$\sum_{K=1}^{\lfloor \frac{n+1}{2} \rfloor} (2K-1) = 2 \times \frac{1}{2} \left\lfloor \frac{n+1}{2} \right\rfloor \left( \left\lfloor \frac{n+1}{2} \right\rfloor + 1 \right) - \left\lfloor \frac{n+1}{2} \right\rfloor$$

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

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

Check $\sum_{\substack{i=1 \\ i \text{ odd}}}^{n=8} i = 1+3+5+7 = 16$

$k = \lfloor \frac{n+1}{2} \rfloor = 4$

$\text{sum} = \left( \lfloor \frac{n+1}{2} \rfloor \right)^2 = \left( \lfloor \frac{9}{2} \rfloor \right)^2 = 4^2 = 16$

Aqil Azmi at 10/1/2020 9:05 AM

$$\sum_{i=0}^{n-1} a = a \times \#\text{terms} = an$$

$$\sum_{i=1}^{n} a = an$$

$$\sum_{i=0}^{n-1} i = 0 + 1 + 2 + 3 + \cdots + (n-1)$$

$$\neq \sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n$$

## summing geometric series

$$\sum_{i=0}^{n} ar^i = a + ar + ar^2 + \cdots + ar^n$$

$$= a(1 + r + r^2 + \cdots + r^n)$$

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

Proof

Let $S = 1 + r + r^2 + \cdots + r^n$

$rS = r + r^2 + r^3 + \cdots + r^{n+1}$

$$rS = \cancel{r} + \cancel{r^2} + r^3 + \cdots \cancel{+} + r^{n+1}$$

$$rS - S = r^{n+1} - 1$$

$$\therefore \quad S = \frac{r^{n+1} - 1}{r - 1} \qquad r \neq 1$$

# Methods of Proof.

if p then q $p \rightarrow q$

p: hypothesis فرضية, إثبات

q: conclusion نتيجة, إثبات

- induction
- Counter example
- Proof by cases
- Direct proof
- indirect proof
- proof by Contradiction

## Direct Proof $p \rightarrow q$

$T \rightarrow T$ assume p is True

show that q is True

Prove "if n is odd, then $n^2$ is odd"

Assume n is odd. Let $n=2k+1$.

So $n^2 = (2k+1)^2 = 4k^2+4k+1$

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

$=$ odd

## Indirect Proof $p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$

Prove "if $3n+2$ is odd then $n$ is odd"

Let $3n+2 = 2k+1 \Rightarrow n = \frac{2k-1}{2}$ ? odd / even

Let $3n+2 = 2k+1 \Rightarrow n = \frac{2k-1}{3}$ ? odd even integer

can't use direct proof

$\neg q$ = "n is even" $\Rightarrow$ let $n = 2k$ $\ni$ k is some integer

So $3n+2 = 3(2k)+2$

$= 6k+2$

$= 2(3k+1)$

$=$ even

$= \neg p$

Aqil Azmi, PhD. at 10/6/2020 9:00AM

## Proof by contradiction

we show $\neg p \rightarrow F$

Example 1 show that $\sqrt{2}$ is irrational. عدد غير كسري

cannot be written as $\frac{a}{b}$ $\ni$ $a, b \in \mathbb{Z}$

Proof assume (opposite).

Let $\sqrt{2} = \frac{a}{b}$ $\ni$ $a, b \in \mathbb{Z}$ $b \neq 0$ in simplest form (no common denomenator) لا يوجد قاسم مشترك

squaring

$2 = a^2/b^2 \Rightarrow a^2 = 2b^2$ = even

$a^2$ even $\Rightarrow$ a even

let $a = 2k$ $k \in \mathbb{Z}$

let $a = 2k$ $k \in \mathbb{Z}$

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

$= 4k^2 = 2b^2 \Rightarrow b^2 = 2k^2$

$b^2$ even $\Rightarrow$ b even

تناقض

we have a contradiction.

a, b both even and we assumed no common denomenator.

So, our assumption is wrong.

Aqil Azmi, PhD. at 10/8/2020 9:09 AM

## Proof by contradiction

① $\neg p \rightarrow F$

② assume p and $\neg q$ both to be true

use indirect proof to show $\neg q \rightarrow \neg p$

$\neg p$ → contradiction

Example 2

show that if $3n+2$ is odd (p) then n is odd (q)

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

n " even ($\neg q$ is True)

now we use the indirect proof $\neg q \rightarrow \neg p$ → contradiction

now we use the indirect proof $\neg q \to \neg p$ contradiction

$n$ even $\Rightarrow$ let $n = 2K$ $\ni$ $K$ is integer

then $3n+2 = 3(2K)+2 = 2(3K+1) = \text{even}$ } $\neg p$ is True

## Proof by cases

Here $p = p_1 \vee p_2 \vee \cdots \vee p_n$

we show $p_1 \to q$, $p_2 \to q$, $\vdots$, $p_n \to q$ } $p \to q$

**Example**

2 = خانة الآحاد

show that an integer ending with 2 cannot be a perfect square

مربع كامل

$n = \ldots\ldots 2$ is not a perfect square

**Proof**

Let $n = 10k + l$ $\quad k \in \{0, 1, 2, 3, \ldots\}$

$l$: 0, 1, 2, ..... 9

$786 = 10 \times 78 + 6$

$35703 = 10 \times 3570 + 3$

**10 cases**

$n^2$ خانة الآحاد

case $l=0$ $\quad n^2 = (10K+0)^2 = 100K^2 + 0$

case $l=1$ $\quad n^2 = (10K+1)^2 = 100K^2 + 20K + 1$

case $l=1$ $\quad m^2=(10k+1)^2 = 100k^2+20k+1$

case $l=2$ $\quad m^2=(10k+2)^2 = 100k^2+40k+4$

case $l=3$ $\quad m^2=(10k+3)^2 = 100k^2+60k+9$

case $l=4$ $\quad m^2=(10k+4)^2 = 100k^2+80k+16$

$= 100k^2+10(8k+1)+6$

continue with cases $l=5,6,7,8,9$

At the end we see that $m^2$ ends with either $0,1,4,5,6,9$. No 2.

Counter example مثال مناقض

"All primes are odd"

2 is even and is prime.

Sunday, October 11, 2020 8:52 AM

# Mathematical Induction

Used to prove propositions of form $\forall n\, P(n)$ where universe of discourse is positive integers

Two steps:

1. Base case: show $P(1)$ is True
2. Inductive case: assume $P(n)$ is True for some $n$. Show that $P(n) \rightarrow P(n+1)$ is also True

$$[P(1) \wedge \forall n\,(P(n) \rightarrow P(n+1))] \rightarrow \forall n\, P(n)$$

## Example 1

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

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

Base case: $n = 1$

LHS $= 1$

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

$P(1)$ is True

Inductive case:

Assume $P(n)$ is True for some $n$, we try to show that $P(n+1)$ is also True

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

$$= \left(\sum_{K=1}^{n} K\right) + (n+1)$$

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

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

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

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

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

From both case $P(n)$ is True for all $n \in \mathbb{Z}^+$

**Example 2** $P(n) =$ "$\sum_{k=m}^{n} k = \frac{1}{2}[n(n+1) - m(m-1)]$"

show that

Base case: $n = m$

LHS $P(m) = m$

RHS $P(m) = \frac{1}{2}[m(m+1) - m(m-1)]$

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

$= m$

$P(n)$ is True

Inductive case

Assume $P(n)$ is True induction الـ فرضية

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

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

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

$= \frac{1}{2}[n(n+1) - m(m-1)]$ by induction hypothesis

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

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

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

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

$=$ RHS of $P(n+1)$

Aqil Azmi, PhD. at 10/13/2020 9:04 AM

Example 3

10/13/2020
9:04 AM

## Example 3

Let $H_k = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k}$

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

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

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

**Base case** $(n = 0)$

LHS $H_1 = 1$
RHS $= 1$
} $P(0)$ is True

**Inductive case**

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

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

$= \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^n}\right) + \frac{1}{2^n+1} + \frac{1}{2^n+2} + \cdots + \frac{1}{2^{n+1}}$

$H_{2^n} \geq 1 + \frac{n}{2}$ by induction hypothesis

$\geq 1 + \frac{n}{2} + \left[\frac{1}{2^n+1} + \frac{1}{2^n+2} + \cdots + \frac{1}{2^{n+1}}\right]$

$= \frac{1}{2^n + 2^n}$

$\geq$ Smallest term $\times$ # terms

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

$= \frac{1}{2}$

$\geq 1 + \frac{n}{2} + \frac{1}{2}$

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

$=$ RHS of $P(n+1)$

## Strong Induction

1. Base case
2. Inductive case
   Assume $P(1), P(2), \ldots, P(n)$ all true

and we show that $P(n+1)$ is also true

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

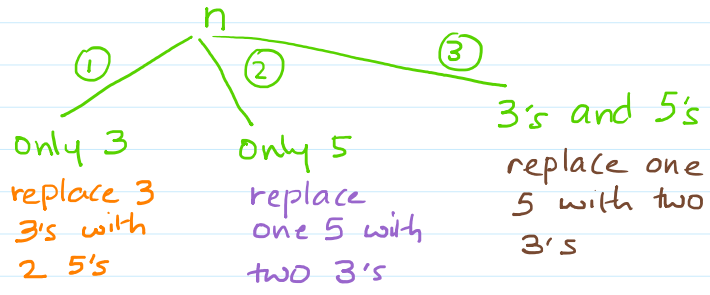
**Example**

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

**Base case** ($n=8$): It is true since $8 = 3+5$

**Inductive case**

We show how to express $n+1$ given $n$




$19 = 3+3+3+5+\cancel{5}$ $3+3$

$20 = 3+3+3+3+3+\cancel{5}$ $3+3$

22

$21 = 3+3+3+3+\cancel{3+3+3}$ $5+5$

$= 3+3+3+3+5+5$

# Integers and division

**Def** $a, b$ are integers $\ni a \neq 0$.

$a \mid b$ "a divides b"

b يقسم a

factor means $b = ac$ for some int. $c$

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

b لا يقسم a

**Example**

$4 \mid 20$ $3 \mid 27$ $6 \mid 30$

$4 \nmid 19$ $3 \nmid 20$ $6 \nmid 33$

**Th**

Let $a, b, c$ be integers. Then

* if $a \mid b$ and $a \mid c$ then $a \mid (b+c)$
* if $a \mid b$ then $a \mid bc$ $\forall$ integer $c$
* if $a \mid b$ and $b \mid c$ then $a \mid c$

**Proof**

* $a \mid b$ then $b = ax$ for some integer $x$

$a|c$ " $c = ay$ " " " $y$

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

integer

therefore $a|(b+c)$

* $a|b \Rightarrow b = ax$ for some integer $x$
so $bc = a(xc)$ integer
therefore $a|bc$

* $a|b \Rightarrow b = ax$ for some integer $x$
$b|c \Rightarrow c = by$ " " " $y$
$= a(xy)$ integer

$\therefore a|c$

عدد أولي

**Def.** A positive integer $p > 1$ is **prime** iff the only positive factors are 1 and $p$.

Ex 7 is prime
9 not prime (composite) i.e $3|9$

**Th** Every positive integer can be written

uniquely as a product of primes

Ex $20 = 2^2 \times 5$

$30 = 2 \times 3 \times 5$

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

$1024 = 2^{10}$

Th

If $n$ is composite then $n$ has a prime divisor $\leq \sqrt{n}$

(means, at least one of the prime divisors is $\leq \sqrt{n}$ )

Proof

$n$ composite $\Rightarrow$ $n = a \times b$ $\ni$ $1 < a \leq b < n$

Claim: either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

if above claim not true, then both $a$ and $b$ are $> \sqrt{n}$.

But $n = a \times b > \sqrt{n} \times \sqrt{n} = n$ not possible

Above theorem gives a way to test if a given number $n$ is prime.

# Primality testing

Given an integer $n$. Is $n$ prime?

Let $p$ = all primes $\leq \lfloor \sqrt{n} \rfloor$.
if none of these primes divides $n$,
then $n$ is prime

# Prime factorization

Given integer $n$. Write all its prime factors.

Express $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ $\exists$ $p_1, p_2, \ldots$ primes
$\alpha_1, \alpha_2 \geq 0$

$$= \prod_{i=1}^{k} p_i^{\alpha_i}$$

How many primes do we have? infinite

**Th** there are infinitely many primes.

**Proof** Assume # primes is finite,
$p_1, p_2, p_3, \ldots, p_n$ (the full list)

Let $x = (p_1 \cdot p_2 \cdot p_3 \cdots p_n) + 1$

x can either be composite or prime.

if x composite then $\exists$ prime p than divides x.

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

(always we have remainder 1)

$\therefore$ x is prime.

So we have infinite many primes.

Ex. Is 103 prime?

$\sqrt{103} = 10.148$

list of primes $\leq \lfloor \sqrt{103} \rfloor = \{2, 3, 5, 7\}$

$2 \nmid 103$, $3 \nmid 103$, $5 \nmid 103$ $7 \nmid 103$

$\therefore$ 103 is prime.

Ex. Find the prime factors of 7007.

$2 \nmid 7007$

$3 \nmid 7007$

$5 \nmid 7007$

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

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

$7 \nmid 143$

$11 \mid 143$ $\quad \frac{143}{11} = 13$

$11 \nmid 13$

$13 \mid 13.$

Prime factors $7007 = 7^2 \times 11 \times 13$

Aqil Azmi, PhD. at 10/20/2020 8:59 AM

Ex. Factorize 9761

$2 \nmid 9761$

$3 \nmid 9761$

$5 \nmid 9761$

$\vdots$

$41 \nmid 9761$

$43 \mid 9761$

$\frac{9761}{43} = 227$ ← this is prime because $43 > \sqrt{227}$

$\therefore 9761 = 43 \times 227$

## Algorithm to factorize n.

```
p ← 2
while ( p ≤ √n ) do
{
    while ( p | n ) do
    {
        print p
        n ← n/p
    }
    p ← next prime
}
if (n ≠ 1) print n
```

## Greatest Common Divisors

**Def.** integers $a, b$.
the largest integer $d$ ∋ $d|a$ and $d|b$ is called greatest common divisor of $a$ and $b$.

القاسم المشترك الأكبر

$d = \gcd(a, b)$ note: $d \geq 1$

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

divisors of 24 : 1, 2, 3, 4, 6, 12
" " 36 : 1, 2, 3, 4, 6, 9, 12, 18

$\gcd(24,36) = 12$

**Def.** integers $a, b$. if $\gcd(a,b) = 1$ we say $a, b$ are relatively prime

**Ex** $\gcd(22,17) = 1$. so $17, 22$ are relatively 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 $10, 17, 21$ pairwise relatively prime?

$\gcd(10,17) = 1$
$\gcd(10,21) = 1$
$\gcd(17,21) = 1$

} YES

**Ex** Are $10, 19, 24$ pairwise relatively prime?

$\gcd(10,19) = 1$
$\gcd(10,24) = 2$
$\gcd(19,24) = 1$

} NO

# How to calculate gcd(a, b).

Let $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ where $p_i$ prime

$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_n^{\beta_n}$ $\alpha_i, \beta_i \geq 0$

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

To show above formula is correct.

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

to show d is the gcd of a, b, we need to prove

① $d \mid a$ and $d \mid b$

② there $\nexists$ $\acute{d} > d$ such that $\acute{d} \mid a$ and $\acute{d} \mid b$

Ex find gcd(24, 36)

$24 = 2^3 \times 3$

$36 = 2^2 \times 3^2$

$\gcd(24, 36) = 2^2 \times 3 = 12$

Ex find gcd(120, 500)

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

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

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

القاسم المشترك الأصغر

Def. The least common multiple of integers $a, b$ is the smallest integer that is divisible by both $a$ and $b$.

$m = \text{lcm}(a, b)$ where $m$ is the smallest number $\ni a|m$ and $b|m$

Aqil Azmi,
PhD. at
10/22/2020
9:08 AM

Calculating lcm(a, b)

Let $a = \prod_{i=1}^{k} p_i^{\alpha_i}$ $b = \prod_{i=1}^{k} p_i^{\beta_i}$ $p_i$ prime $\alpha_i, \beta_i \geq 0$

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

Ex. find lcm(24,30)

$2^3 \times 3$ $2 \times 3 \times 5$

$$\text{lcm}(24,30) = 2^3 \times 3 \times 5 = 120$$

**Th** Integers $a, b > 0$ then

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

**Proof**

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

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

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

$$= \alpha_i + \beta_i$$

$$= \prod_{i=1}^{k} p_i^{\alpha_i + \beta_i}$$

$$= \prod_{i=1}^{k} p_i^{\alpha_i} \cdot p_i^{\beta_i}$$

$$= a \times b$$

# Modular Arithmetic

**Def.** Let $a, m$ integers, $m > 0$

We denote the unique remainder of $\frac{a}{m}$ by $a \bmod m$.

**Note:** $a \bmod m$ is $r$ $\exists$ $a = qm + r$ and $0 \le r < m$

($r$: unique)

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

$16 \bmod 8 = 0$

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

**Def.** $a, b$ integers, $m > 0$ then

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

$a$ is congruent to $b$ modulo $m$

يطابق في

**Note:**

$$a \equiv b \bmod m \iff a \bmod m = b \bmod m \quad (*)$$

$a \not\equiv b \bmod m \iff a \bmod m \neq b \bmod m$

Ex. $17 \equiv 5 \bmod 6$ ? Yes, $6 \mid (17-5)$

$24 \equiv 14 \bmod 6$ ? No, $6 \nmid (24-14)$

$30 \not\equiv 5 \bmod 7$ ? Yes, $7 \nmid (30-5)$

Proof.

To prove (*) we need to show it is true both ways

① $a \equiv b \bmod m \Rightarrow a \bmod m = b \bmod m$

② $a \bmod m = b \bmod m \Rightarrow a \equiv b \bmod m$

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

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

$\Rightarrow a = b + mk$

taking modulo $m$ of both sides,

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

[2] now $a \bmod m \Rightarrow a = mq_1 + r_1$

$b \bmod m \Rightarrow b = mq_2 + r_2$

Since $a \bmod m = b \bmod m \Rightarrow r_1 = r_2$.

Hence,

$$a - b = m(q_1 - q_2) \quad \text{or} \quad m \mid (a-b)$$

$$\Rightarrow a \equiv b \bmod m$$

Next, we need to show

③ $a \not\equiv b \bmod m \Rightarrow a \bmod m \neq b \bmod m$

④ $a \bmod m \neq b \bmod m \Rightarrow a \not\equiv b \bmod m$

③ given $a \not\equiv b \bmod m \Rightarrow m \nmid (a-b)$

So, $a - b = mq + r \quad \exists \quad 0 < r < m$

$$a = b + mq + r$$
$$= b + r + mq$$

take mod m of both sides

$$a \bmod m = (b+r) \bmod m$$
$$\neq b \bmod m$$

④ Given $a \bmod m \neq b \bmod m$,

so let

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

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

$\neq 0$

So, $m \nmid (a-b)$

$\therefore a \not\equiv b \bmod m$

**Th.** Let $m > 0$, then

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

Some integer ↓

**Proof.**

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

or, $a = b + km$

while, if $a = b + km \Rightarrow a - b = km$

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

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

$a + c \equiv b + d \bmod m$

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

**Proof.**

Let $a = b + k_1 m$

$c = d + k_2 m$ $\qquad k_1, k_2 \in \mathbb{Z}$

then, $a + c = b + d + m(k_1 + k_2)$

So, $m \mid ((a+c) - (b+d))$

or $a + c \equiv b + d \mod m$

Similarly we can show $ac \equiv bd \mod m$

Th. Let $a = bq + r$ $\exists$ $a, b, q, r$ are integers and $0 \leq r < b$

then

$$\gcd(a, b) = \gcd(b, r)$$

Proof.

if $d \mid a$ and $d \mid b$ then $d \mid (xa \pm yb)$

$\exists$ $x, y \in \mathbb{Z}$

let $x = 1$, $y = q$,

then $d \mid (a - bq)$ $\Rightarrow$ $d \mid r$

$= r$

meaning, if $d \mid a$ and $d \mid b$ then $d \mid r$.

That is, the common divisors of $a, b, r$ are the same.

## Euclidean Algorithm for gcd

# Euclidean Algorithm for gcd

Ex. find gcd(287, 91)

$287 = \boxed{3} \times 91 + \boxed{14} \Rightarrow \gcd(287,91) = \gcd(91,14)$

$91 = \boxed{6} \times 14 + \boxed{7} \Rightarrow \gcd(91,14) = \gcd(14,7)$

$14 = \boxed{2} \times 7 + \boxed{0}$ ← This is gcd(287, 91)

Aqil Azmi, PhD. at 11/3/2020 9:01 AM

## Pseudo Code of Euclidean Algorithm

```
procedure gcd(a,b)      // a ≥ b
{
    pick r ∋ a = bq + r     where 0 ≤ r < b
    if (r > 0) return gcd(b, r)
    return b                    // final result
}
```

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

$$\gcd(a,b) = sa + tb$$

(expressing gcd as linear combination of its arguments)

Ex Express $\gcd(252, 198)$ as linear combination of both numbers.

$$\gcd(252, 198) = \boxed{?} \times 252 + \boxed{?} \times 198$$

Steps: ① use Euclidean to find $\gcd(a, b)$
② go backward (bottom to top)

$$252 = \boxed{1} \times 198 + \boxed{54}$$
$$198 = \boxed{3} \times 54 + \boxed{36}$$
$$54 = \boxed{1} \times 36 + \boxed{18} \leftarrow \gcd$$
$$36 = \boxed{2} \times 18 + \boxed{0}$$

We want to express $\gcd(252, 198) = 18$ as linear combination of 252 and 198

$$18 = 54 - 1 \times 36$$

$$= 54 - 1 \times (198 - 3 \times 54)$$
$$= -1 \times 198 + 4 \times 54$$

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

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

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

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

**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 $c$

$\Rightarrow sac + tbc = c$

$sac$: divisible by $a$

$tbc$: divisible by $a$ (due to $a \mid bc$)

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

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

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

if $ac \equiv bc \bmod m$ and $\gcd(c, m) = 1$ } $a \equiv b \bmod m$

**Proof** Given $ac \equiv bc \bmod m$

So, $m \mid (ac - bc)$

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

but $m \nmid c$ (since they are relatively prime)

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

# Modular Arithmetic

**Def.** Let $a$, $m$ integers, $m > 0$

We denote the unique remainder of $\frac{a}{m}$ by $a \bmod m$.

**Note:** $a \bmod m$ is $r$ $\exists$ $a = qm + r$ and $0 \le r < m$

($r$: unique)

**Ex**

$17 \bmod 5 = 2$ $\quad 17 = 3 \times 5 + 2$

$16 \bmod 8 = 0$

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

**Def.** $a, b$ integers, $m > 0$ then

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

$a$ is congruent to $b$ modulo $m$

يطابق

**Note:**

$$a \equiv b \bmod m \iff a \bmod m = b \bmod m \quad (*)$$

$$a \not\equiv b \bmod m \iff a \bmod m \neq b \bmod m$$

Ex. $17 \equiv 5 \bmod 6$ ? Yes, $6 \mid (17-5)$

$24 \equiv 14 \bmod 6$ ? No, $6 \nmid (24-14)$

$30 \not\equiv 5 \bmod 7$ ? Yes, $7 \nmid (30-5)$

Proof.

To prove (*) we need to show it is true both ways

① $a \equiv b \bmod m \Rightarrow a \bmod m = b \bmod m$

② $a \bmod m = b \bmod m \Rightarrow a \equiv b \bmod m$

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

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

$\Rightarrow a = b + mk$

taking Modulo m of both sides,

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

[2] now $a \bmod m \Rightarrow a = mq_1 + r_1$

$b \bmod m \Rightarrow b = mq_2 + r_2$

Since $a \bmod m = b \bmod m \Rightarrow r_1 = r_2$.

Hence,

$a - b = m(q_1 - q_2)$ or $m \mid (a-b)$

$\Rightarrow a \equiv b \bmod m$

Next, we need to show

③ $a \not\equiv b \bmod m \Rightarrow a \bmod m \neq b \bmod m$

④ $a \bmod m \neq b \bmod m \Rightarrow a \not\equiv b \bmod m$

[3] given $a \not\equiv b \bmod m \Rightarrow m \nmid (a-b)$

So, $a - b = mq + r \quad \exists \quad 0 < r < m$

$$a = b + mq + r$$
$$= b + r + mq$$

take mod m of both sides

$$a \bmod m = (b+r) \bmod m$$
$$\neq b \bmod m$$

[4] Given $a \bmod m \neq b \bmod m$,

So let

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

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

So, $m \nmid (a-b)$

$\therefore a \not\equiv b \bmod m$

**Th.** Let $m > 0$, then

$$a \equiv b \bmod m \iff \exists \text{ integer } k \ni a = b + km$$

Some integer ↓

**Proof.**

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

or, $a = b + km$

while, if $a = b + km \Rightarrow a - b = km$

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

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

$$a + c \equiv b + d \bmod m$$

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

**Proof.**

Let $a = b + k_1 m$

$c = d + k_2 m$ $\qquad k_1, k_2 \in \mathbb{Z}$

then, $a + c = b + d + m(k_1 + k_2)$

so, $m \mid ((a+c) - (b+d))$

or $a + c \equiv b + d \bmod m$

Similarly we can show $ac \equiv bd \mod n$

**Th.** Let $a = bq + r$ $\exists$ $a, b, q, r$ are integers and $0 \le r < b$

then

$$\gcd(a, b) = \gcd(b, r)$$

**Proof.**

if $d \mid a$ and $d \mid b$ then $d \mid (xa \pm yb)$

$\exists$ $x, y \in \mathbb{Z}$

let $x = 1$, $y = q$,

then $d \mid (a - bq) \Rightarrow d \mid r$

($a - bq = r$)

meaning, if $d \mid a$ and $d \mid b$ then $d \mid r$.

That is, the common divisors of $a, b, r$ are the same.

## Euclidean Algorithm for gcd

Ex. find $\gcd(287, 91)$

$287 = \boxed{3} \times 91 + \boxed{14} \Rightarrow \gcd(287, 91) = \gcd(91, 14)$

$91 = \boxed{6} \times 14 + \boxed{7} \Rightarrow \gcd(91, 14) = \gcd(14, 7)$

$91 = \boxed{6} \times 14 + \boxed{7} \Rightarrow \gcd(91,14) = \gcd(14,7)$

$14 = \boxed{2} \times 7 + \boxed{0}$ ← this is $\gcd(287,91)$

Aqil Azmi, PhD. at 11/3/2020 9:01 AM

## Pseudo Code of Euclidean Algorithm

```
procedure gcd(a,b)      // a ≥ b
{
    pick r ∋ a = bq + r     where 0 ≤ r < b
    if (r > 0) return gcd(b,r)
    return b                          // final result
}
```

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

$$\gcd(a,b) = sa + tb$$

(expressing gcd as linear combination of its arguments)

**Ex** Express gcd(252, 198) as linear combination of both numbers.

$$\gcd(252,198) = \boxed{?} \times 252 + \boxed{?} \times 198$$

Steps: ① use Euclidean to find gcd(a,b)

② go backward (bottom to top)

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

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

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

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

We want to express $\gcd(252, 198) = 18$ as linear combination of 252 and 198

$18 = 54 - 1 \times 36$

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

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

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

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

$\therefore \gcd(252, 198) = 18$

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

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 $c$

$\Rightarrow$ $sac + tbc = c$

$sac$: divisible by $a$

$tbc$: divisible by $a$ (due to $a \mid bc$)

So $a \mid (sac + tbc) \Rightarrow a \mid c$

($sac + tbc = c$)

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

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

if $ac \equiv bc \bmod m$ and $\gcd(c, m) = 1$ } $a \equiv b \bmod m$

**Proof** Given $ac \equiv bc \bmod m$

So, $m \mid (ac - bc)$

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

but $m \nmid c$ (since they are relatively prime)

$\therefore$ $m \mid (a - b)$ or $a \equiv b \bmod m$

Aqil Azmi, PhD. at 11/5/2020 9:02 AM

**Th** if $a, m$ are relatively prime. Then there exist a unique integer $\hat{a} < m$ such that

$$a \times \hat{a} \equiv 1 \mod m.$$

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

**Proof** Since $\gcd(a, m) = 1$

$\Rightarrow$ there exist $s, t \ni sa + tm = 1$

Now mod $m$ of both sides,

$$sa + tm \equiv 1 \mod m.$$

But $m \mid tm \Rightarrow sa \equiv 1 \mod m$

↑ this is the inverse of $a$ in modulo $m$

**Ex.**

Find the inverse of 4 in modulo 7.

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

Now $4 \times 2 = 8 \equiv 1 \mod 7$

$\therefore$ 2 is the inverse of 4 in mod 7.

Table of inverses in modulo 7

| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| inverse | 1 | 4 | 5 | 2 | 3 | 6 |

Table of inverses in modulo 8

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| inverse | 1 | – | 3 | – | 5 | – | 7 |

↖ no inverse since $\gcd(8,6) \neq 1$

Table of inverses in modulo 9

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| inverse | 1 | 5 | – | 7 | 2 | – | 4 | 8 |

Solve $4x \equiv 3 \mod 9$ $x$ is integer.

$=$

find the value of $x$ that satisfy the equation

This equation has a unique solution since 4 and 9 are relatively prime.

$x \equiv 3 \times \underbrace{(\text{inverse of } 4 \text{ in modulo } 9)}_{=7} \mod 9$

$x \equiv 3 \times 7 \mod 9$

$\equiv 21 \mod 9$

$\equiv 3 \mod 9$

↑ unique solution

General solution $x = 3 + 9k$ for $k \in \mathbb{Z}$

This means we have infinite solutions

$x = \{ \ldots, -6, 3, 12, 21, 30, \ldots \}$

Ex.

Solve $22x \equiv 3 \mod 51$

are relatively prime. Inverse exist

$X \equiv 3 \times$ (inverse of 22 in modulo 51) $\mod 51$

to find inverse express the $\gcd(51, 22) = 1$ using the linear combination.

$51 = \boxed{2} \times 22 + \boxed{7}$

$22 = \boxed{3} \times 7 + \boxed{1}$ ← gcd

next, $1 = 22 - 3 \times (7)$

$= 22 - 3 \times (51 - 2 \times 22)$

$= -3 \times 51 + (7) \times 22$

↑ inverse of 22 in modulo 51

$X \equiv 3 \times 7 \mod 51$

$\equiv 21 \mod 51$

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

Aqil Azmi, PhD. at 11/8/2020 9:03 AM

Ex. Solve $4x^2 \equiv 2 \mod 11$

Ex. Solve $4x^2 \equiv 2 \mod 11$

relatively prime

So, $x^2 \equiv 2 \times$ (inverse of 4 in modulo 11) $\mod 11$

① use Euclidean to find gcd. then express as linear combination

② by trial & error

$\equiv 2 \times 3 \mod 11$

$\equiv 6 \mod 11$

Is there a solution for $x^2 \equiv 6 \mod 11$?

| x | $x^2$ | $x^2 \mod 11$ |
|---|---|---|
| 1 | 1 | 1 |
| 2 | 4 | 4 |
| 3 | 9 | 9 |
| 4 | 16 | 5 |
| 5 | 25 | 3 |
| 6 | 36 | 3 |
| 7 | 49 | 5 |
| 8 | 64 | 9 |
| 9 | 81 | 4 |
| 10 | 100 | 1 |

Since 6 not in list, so $x^2 \equiv 6 \mod 11$ has no solution

Ex Consider the equations. Solve,

solutions

$x \equiv 2 \mod 5 \Rightarrow 2, 7, 12, 17, 22, 27, 32, 37, 42, \ldots$

$x \equiv 1 \mod 8 \Rightarrow 1, 9, 17, 25, 33, 41, \ldots$

Common Solution

$\therefore$ $x = 17$ Solves both equation

## Th Chinese Remainder Theorem (CRT)

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

Then
$$x \equiv a_1 \bmod m_1$$
$$x \equiv a_2 \bmod m_2$$
$$\vdots$$
$$x \equiv a_k \bmod m_k$$

has a unique solution modulo $m_1 \cdot m_2 \cdots m_k$.

The solution $x$ is $0 \le x < \prod_{i=1}^{k} m_i$

Ex Solve ($a_1$, $m_1$)
$$x \equiv 2 \bmod 3$$
($m_2$)
$$x \equiv 3 \bmod 5$$
($m_3$, $a_3$)
$$x \equiv 2 \bmod 7$$

We have a unique solution since 3, 5, 7 are pairwise relatively prime.

Let $m = 3 \times 5 \times 7 = 105$

$$M_1 = \frac{m}{3} = 35$$

$M_2 = \frac{m}{5} = 21$

$M_3 = \frac{m}{7} = 15$

Solution $x = a_1 \cdot M_1 \cdot y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \mod m$

inverse of $M_1$ in modulo $m_1$

inverse of $M_3$ in modulo $m_3$
i.e $M_3 y_3 \equiv 1 \mod m_3$

By trial & error

$y_1 = 2$ Since $35 \times 2 \equiv 1 \mod 3$

$y_2 = 1$ " $21 \times 1 \equiv 1 \mod 5$

$y_3 = 1$ " $15 \times 1 \equiv 1 \mod 7$

$\therefore x \equiv 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 \mod 105$

$\equiv 233 \mod 105$

$\equiv 23 \mod 105$

General solution $x = 23 + 105k \quad k \in \mathbb{Z}$

Aqil Azmi, PhD. at 11/10/2020 9:05 AM

Th. Fermat's Little Theorem

if $p$ is prime and $p \nmid a$ then

$a^{p-1} \equiv 1 \mod p$, or $a^r \equiv a \mod p$

Proof.

Let $p \nmid a$

List first $p-1$ multiples of $a$,

$a, 2a, 3a, 4a, \ldots, (p-1)a$

all these are distinct modulo $p$,

otherwise, say $ra \equiv sa \mod p \Rightarrow r \equiv s \mod p$

Multiply them,

$a \times 2a \times 3a \times \cdots \times (p-1)a$

these are distinct and must be congruent to $1, 2, \ldots, p-1$ in some order

so, $a^{p-1}(p-1)! \equiv (p-1)! \mod p$

$a^{p-1} \equiv 1 \mod p$

Th Euler's Generalization

if $a$ and $n$ are relatively prime, then

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

where $\phi(n)$ is Euler's totient function, which is numbers $< n$ that are relatively prime to $n$.

Mathematically,

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

Ex.

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

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

In general, if $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ then

($p_1, p_2, \ldots, p_k$: primes)

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

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

Ex.

$12 = 2^2 \times 3$

$$\phi(12) = 12 \cdot \left(\frac{2-1}{2}\right) \cdot \left(\frac{3-1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$$

$15 = 3 \times 5$

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

NOTE: $\phi(p) = p - 1$ where $p$ is prime. That is why Euler is generalization of Fermat's Little theorem.

Ex.

Recall 97 is prime. $25^{96} \equiv 1 \bmod 97$ (Fermat)

$25^{192} = (25^{96})^2 \equiv 1^2 \bmod 97 \equiv 1 \bmod 97$

Suppose we want to calculate $25^{1203} \bmod 97$

According to Fermat, $25^{1152} = (25^{96})^{12} \equiv 1 \bmod 97$,

So $25^{1203} \equiv 25^{1152} \times 25^{51} \bmod 97$

$\equiv 1 \bmod 97$

$\equiv 25^{51} \bmod 97$

Using Fast Exponentiation technique,

Aqil Azmi, PhD. at 11/12/2020 9:08 AM

$25 \bmod 97 \equiv 25$

$25^2 \bmod 97 \equiv 43$

$25^4 \bmod 97 \equiv 43^2 \bmod 97 \equiv 6$

$25^8 \bmod 97 \equiv 6^2 \bmod 97 \equiv 36$

$25^{16} \bmod 97 \equiv 36^2 \bmod 97 \equiv 35$

$25^{32} \bmod 97 \equiv 35^2 \bmod 97 \equiv 61$

Now $25^{51} = 25^{32} \times 25^{16} \times 25^2 \times 25$

So, $25^{51} \equiv 61 \times 35 \times 43 \times 25 \bmod 97 \equiv 8$

Hence $25^{1203} \bmod 97 \equiv 8$

Ex. Suppose we want $27^{1203} \bmod 100$

Can't use Fermat since 100 not- prime.
We can use Euler since 27 and 100 are relatively prime.

$\phi(100) = 40$

Euler: $27^{\phi(100)} \equiv 1 \bmod 100$

$27^{40} \equiv 1 \bmod 100$

So, $(27^{40})^{30} = 27^{1200} \equiv 1 \bmod 100$

then $27^{1203} = 27^{1200} \times 27^3$

$\equiv 1 \times 27^3 \bmod 100 \equiv 83$

## Public Key CryptoSystem


$P_B$ public key

$S_B$ Secure (secret) key

$S_B$ and $P_B$ cancels each other

① Secure messaging M

A send B message $P_B(M)$

B reads message $S_B(P_B(M)) = M$

② Authentication التوثيق

A sends B message $\acute{M} = S_A(P_B(M))$

B recovers message $S_B(P_A(\acute{M}))$

RSA cryptosystem.

① Let $n = p \times q$ ($p, q$ large primes)

② pick $e$ $\ni$ $\gcd(e, (p-1)(q-1)) = 1$

③ compute $d$ $\ni$ $de \equiv 1 \mod (p-1)(q-1)$

$d$: Secure key

$e$: public key

$M$ = original message

$C$ = cipher text

Then

$C = M^e \mod n$ encryption

$M = C^d \mod n$ decryption

Sunday, November 15, 2020 9:27 AM

# Combinatorics

## Basic Counting principles

### Sum rule

Do task $T_1$ or $T_2$ (but not both)

$\#\text{ways} = |T_1| + |T_2|$

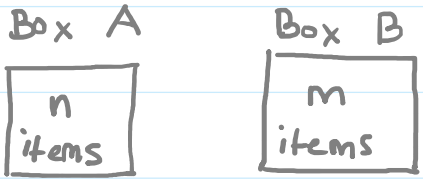
$|T_1|$: # ways to do task $T_1$

### Product rule

Do task $T_1$ and $T_2$

$\#\text{ways} = |T_1| \times |T_2|$

Ex.

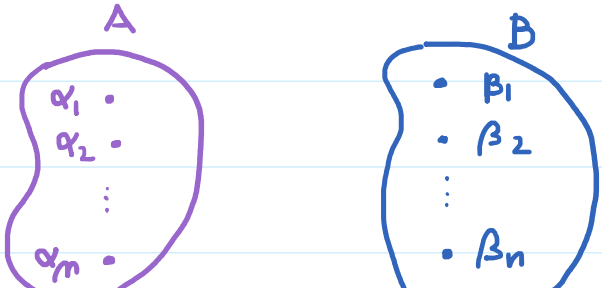


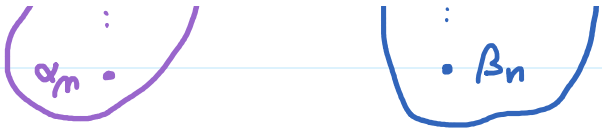

Sum rule: pick one item only from either box A or box B = $n+m$ choices

Product rule: pick one item only from each box = $n \times m$ choices

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

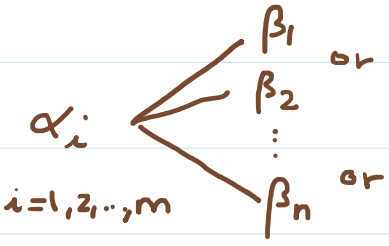
$f: A \to B$






Each of the $\alpha$ in set A has n choices

$\alpha_1$ has n choices
$\alpha_2$ " " "
$\alpha_m$ " " "




Product rule = $n^m$ functions

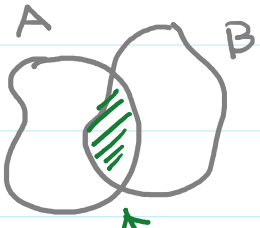
Aqil Azmi, PhD. at 11/17/2020 9:02 AM

## Principle of inclusion-exclusion

Overcounting ⇒ remove (subtract) these elements

undercounting ⇒ add these elements

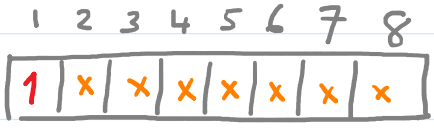
Ex.



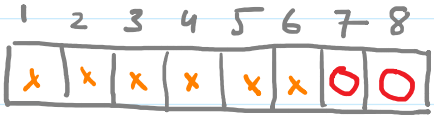

Counted twice

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

Ex. How many bit strings of length 8 either start with a 1 bit or ends w/ two 00

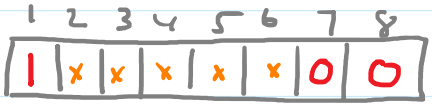



or



can be done in $2^7$ ways

can be done in $2^6$ ways




this pattern counted twice

can be done in $2^5$ ways

# bit strings $= 2^7 + 2^6 - 2^5 = 160$

## 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. Class with 13 students. 2+ must be born in the same month.

Th Generalized Pigeonhole

if $N$ objects are placed into $k$ boxes, then there is at least one box having

at least $\lceil N/k \rceil$ objects.

Proof:

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

$$\#\text{ objects} \leq k \cdot (\lceil N/k \rceil - 1)$$
$$< k \cdot (((N/k) + 1) - 1) = N$$

A contradiction, since we have exactly N objects

NOTE: $\lceil N/k \rceil < (N/k) + 1$

in general: $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1 \qquad x \in \mathbb{R}$

Ex. Suppose we have 10 black, 10 brown, 10 blue and 10 white socks. All mixed up. How many socks to pick (blindly) to guarantee two of same color.

Pick 5 socks.

= Smallest N such that $\lceil \frac{N}{4} \rceil = 2$ (want two socks of same color; $\frac{N}{4}$: # colors)

How many socks to pickup so we have 2 black.

Pick 32 socks

Worst case scenario: 1st 10 are all brown

2nd " " " blue

3rd " " " white

Aqil Azmi, PhD. at 11/22/2020 9:09 AM

Ex. Given set of numbers: $1, 2, 3, \ldots, 25$.

Pick any 14. Show there are at least two numbers who sum 26.

$1 \quad 2 \quad 3 \quad 4 \quad \ldots \quad 11 \quad 12 \quad 13$

$25 \quad 24 \quad 23 \quad 22 \quad \ldots \quad 15 \quad 14$

$26 \quad 26 \quad 26 \quad 26 \qquad 26 \quad 26$

have 12 pairs that sum 26

## Permutation & Combination

**Def.** A permutation of set of distinct objects is an ordered arrangement of these objects (order matters)

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

$$P(n,r) = \underbrace{n(n-1)(n-2)\times\cdots\times(n-r+1)}_{r \text{ terms}}$$

**Proof.**

First element can be chosen in n ways

Second " " " " " n-1 "

consequently,

$$\underbrace{n}_{1^{st}} \quad \underbrace{(n-1)}_{2^{nd}} \quad \cdots \quad \underbrace{(n-r+1)}_{r\text{-th}}$$

We use product rule (since we want to choose all r objects at the same time)

$$P(n,r) = \prod_{k=0}^{r-1} (n-k) = \frac{n!}{(n-r)!}$$

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

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

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

Ex. We have 3 students: Ahmad, Ali, Omar.

Want to give 2 prizes. First = watch, second = pen.

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

| | 1st prize | 2nd prize. | |
|---|---|---|---|
| 1 | Ahmad | Ali | |
| 2 | " | Omar | (notice here |
| 3 | Ali | Ahmad | order matters) |
| 4 | " | Omar | |
| 5 | Omar | Ahmad | |
| 6 | " | Ali | |

Ex. Given 3 colored balls (red, white, black). Pick 2 balls out of 3.

# choices = $\binom{3}{2} = 3$

| | Red | White | Black | |
|---|---|---|---|---|
| 1 | x | x | | (Here order did |
| 2 | x | | x | not matter) |
| 3 | | x | x | |

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

Aqil Azmi, PhD. at 11/24/2020 9:03 AM

= $\binom{10}{3}$ order does not matter since we are

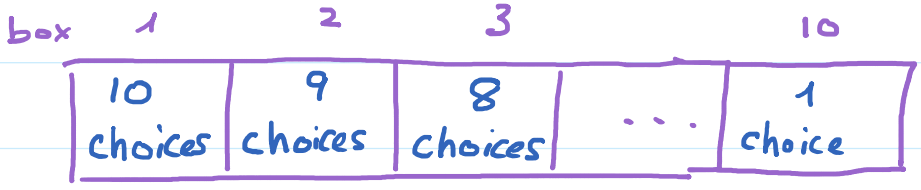
$= \binom{10}{3}$ order does not matter since we are picking 3 zeros (i.e. 3 identical items)

Ex. Repeat, has at least 3 zeros

= # bit strings with 3 zeros
+ # " " " 4 "
⋮
+ # " " " all zeros

$= \sum_{k=3}^{10} \binom{10}{k}$ (we use sum rule)

Ex. How many ways to arrange 10 books




Using product rule $= 10 \times 9 \times 8 \times \cdots \times 1 = 10!$

Ex. Suppose we have 10 books, such that 3 books on math, 3 books on CS, and 4 books on Arabic. Arrange books so one subject books will be together.

$= 3! \times 3! \times 4! \times 3!$ ← # ways to arrange by subject MCA MAC

$= 3! \times 3! \times 4! \times 3!$ ← by subject MCA MAC ⋮

- $3!$: # ways to arrange math books
- $3!$: # ways to arrange CS books
- $4!$: # ways to arrange Arabic books

Aqil Azmi, PhD. at 11/26/2020 8:59 AM

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

$\boxed{5|4|3}$ $P(5,3)$ × $\binom{5}{3} \times 3!$

- $\binom{5}{3}$: selecting 3 out of 5
- $3!$: arranging them

Ex. Do, but one person must be in each picture.

$\boxed{1|4|3} \times 3$ $P(4,2) \times \binom{3}{1}$ × $\binom{4}{2} \times 3!$

- $\binom{3}{1}$: where to place that must picture person
- $\binom{4}{2}$: selecting 2 out of 4
- $3!$: arranging them

Ex. Computer password of length 6-8 characters. Character are either lowercase letter or numeral. Each password must have at least one digit.

$$\#\text{ passwords} = P_6 + P_7 + P_8$$

$$P_6 = \binom{6}{1} \times 10 \times 26^5 + \binom{6}{2} \times 10^2 \times 26^4 + \cdots + \binom{6}{6} \times 10^6$$

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

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

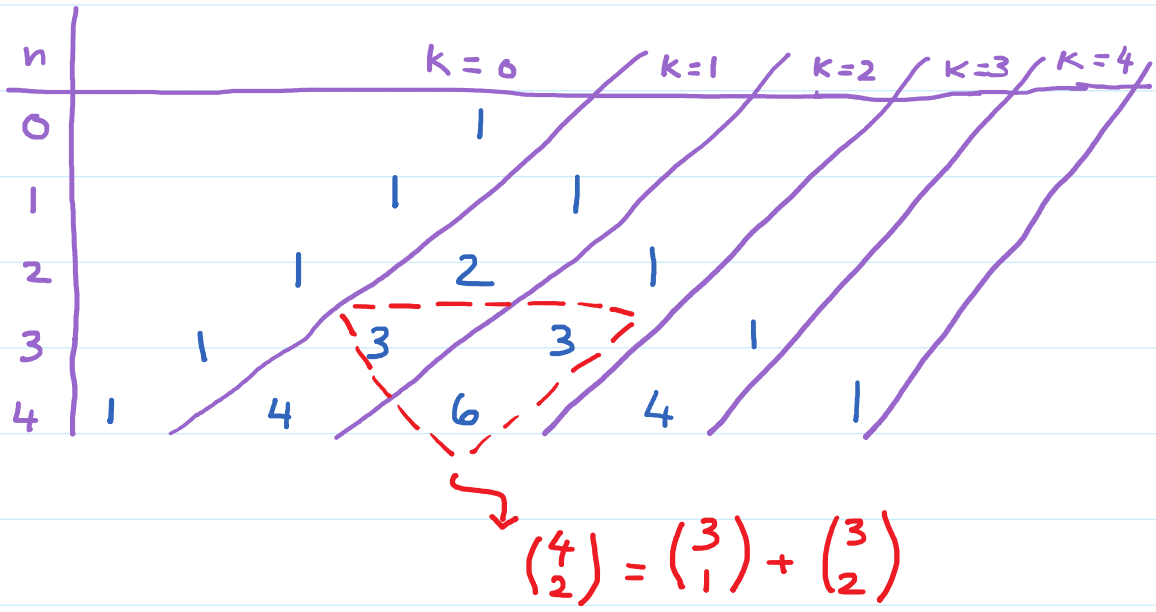
$36^6$: no restriction; $26^6$: just letters

Similarly $P_7$ and $P_8$.

## Binomial Coefficient

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

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




**Th** Let $n$ be positive integer, then

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

**Th** Vandermonde's identity

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

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

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

**Proof.** Use Vandermonde's identity with $m = n = r$ and $\binom{n}{n-k} = \binom{n}{k}$.

**Th. Binomial Theorem**

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

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

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

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

Ex. $(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$

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

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} \cdot 1^k = \sum_{k=0}^{n} \binom{n}{k}$$

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

Proof use Binomial theorem, let $x = 1$, $y = -1$.

Ex. Find coeff of $x^{12}$ in $\left(3x - \frac{5}{x^2}\right)^{30}$

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

$$\sum_{k=0}^{30} \underbrace{\binom{30}{k} \cdot 3^k \cdot x^k \cdot (-5)^{30-k} \cdot (x^2)^{30-k}}_{x^{k-60+2k} = x^{3k-60}}$$

We 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 $n$ positive integer, then

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

such that

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

**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. $(x+y+z)^2 = \sum \frac{2!}{a! \cdot b! \cdot c!} x^a y^b z^c$

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

| a | b | c | |
|---|---|---|---|
| 0 | 0 | 2 | $= z^2$ ← $\frac{2!}{0!\cdot 1!\cdot 1!} = 2$ |
| 0 | 1 | 1 | $+ 2yz$ |
| 0 | 2 | 0 | $+ y^2$ |
| 1 | 0 | 1 | $+ 2xz$ |
| 1 | 1 | 0 | $+ 2xy$ |
| 2 | 0 | 0 | $+ x^2$ |

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

Aqil Azmi, PhD. at 12/1/2020 9:18 AM

Ex. What is the coeff. of $x^5$ in the expansion of $(2x + 3x^2 + 4/x)^5$

$$(2x+3x^2+4/x)^5 = \sum_{n_1+n_2+n_3=5} \frac{5!}{n_1!\cdot n_2!\cdot n_3!} \cdot (2x)^{n_1}\cdot(3x^2)^{n_2}\cdot(4/x)^{n_3}$$

$$2^{n_1}\cdot 3^{n_2}\cdot 4^{n_3}\cdot x^{n_1+2n_2-n_3}$$

want $= x^5$

We want $n_1 + 2n_2 - n_3 = 5$ and $n_1 + n_2 + n_3 = 5$

Solving we get $n_2 = 2n_3$ or $n_1 + 3n_3 = 5$

| $n_1$ | $n_2 = 2n_3$ | $n_3$ |
|---|---|---|
| 5 | 0 | 0 |
| 2 | 2 | 1 |

$$\text{Coeff of } x^5 = 2^5 + \frac{5!}{2! \cdot 2! \cdot 1!} \cdot 2^2 \cdot 3^2 \cdot 4^1 = 4352$$

## Generalized Permutation and Combination

- r- permutation

  Select r object out of n objects such that order matters

  - w/o repetition (بدون تكرار): $P(n,r) = \frac{n!}{(n-r)!}$
  - w/ repetition (مع التكرار): $n^r$

Ex. # words of length k Formed from English alphabet?

if each letter is different = $P(26,k)$

" letters can be used more than once $= 26^k$

| 1 | 2 | | k |
|---|---|---|---|
| 26 | 26 | - - - - | 26 |

- r-combination

  Pick any r objects out of n objects such that order not important

  w/o rep. بدون تكرار

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

  w/ rep. مع التكرار

  $$\binom{n+r-1}{r} \quad \ni \quad r \geq 0$$

Ex. 10 oranges

10 apples

10 banana

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

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

Ex. How many solutions does eq.

$x + y + z = 11$

have such that $x, y, z \geq 0$

# Solutions corresponds to # ways of selecting 11 items from a set of 3 elements, so x items of type 1, y items of type 2, etc.

Think 3 different kind of fruits. Pick 11.

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

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

Aqil Azmi, PhD. at 12/3/2020 9:09 AM

Ex. Suppose $x + y + z = 11$. Want # integer solutions with constraint $x \geq 1$, $y \geq 2$ and $z \geq 4$.

Idea: imagine solving $(\acute{x}+1) + (\acute{y}+2) + (\acute{z}+4) = 11$ such that $\acute{x}, \acute{y}, \acute{z} \geq 0$.

$\Rightarrow$ Find # solutions to $\acute{x} + \acute{y} + \acute{z} = 11 - (1+2+4) = 4$

$\therefore$ solving with $n = 3$, $r = 4$

$$\# \text{ Solutions} = \binom{3 + 4 - 1}{4} = \binom{6}{4} = 15$$

Ex. Find # solutions to $5 \le x+y+z \le 11$

where $x, y, z \ge 0$.

$$= \#\text{ Solutions of } x+y+z = 5$$
$$+ \text{ " " " } x+y+z = 6$$
$$\vdots$$
$$+ \text{ " " " } x+y+z = 11$$

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

## Permutations with indistinguishable objects.

Ex. # different strings can be made by re-ordering letters of SUCCESS

$n = 7$ (# letters)

$n_C = 2$, $n_S = 3$

$$\#\text{ Strings} = \frac{n!}{n_C! \times n_S!} = \frac{7!}{2! \times 3!} = 420$$

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

① # words of length = 5 (duplicates allowed) $= 5^5$

② # " " " $= 4$ (dup. ok) $= 5^4$

③ # " " " = 5 (each letter once) = $5!$

④ # " " " = 4 ( " " " ) = $P(5,4)$

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

⑥ # words " " = 5 (each letter once)

and A, B are together = $4! \times 2!$

حرف مركب (X), C, D, E

AB BA

⑦ # words of length = 5 (each letter once)

and A, B are not together = $5! - 4! \times 2!$

⑧ # words of length = 5 (each letter once)

and letters A, B, C are together = $3! \times 3!$

(حرف مركب) X, D, E

ABC
ACB
⋮
CBA

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

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

Check: 6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96

Ex. Count # integers between 1 and 100 that are

divisible by 12 and 18

$$= \left\lfloor \frac{100}{\text{lcm}(12,18)} \right\rfloor = \left\lfloor \frac{100}{36} \right\rfloor = 2 \quad \text{(i.e. 36, 72)}$$

Aqil Azmi, PhD. at 12/6/2020 9:04 AM

Ex. Do, but count # integers that are divisible by 12 or 18.

= # of those divisible by 12

+ # " " " by 18

− # " " " by 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 100 and 200 that are divisible by 6

$$= \left\lfloor \frac{200}{6} \right\rfloor - \left\lfloor \frac{99}{6} \right\rfloor$$

## Advanced Counting Techique

# Recurrence Relation (RR)

Ex. # bacteria in a colony double every hour. If we have 5 bacteria, how many after n hours?

Recurrence Relation

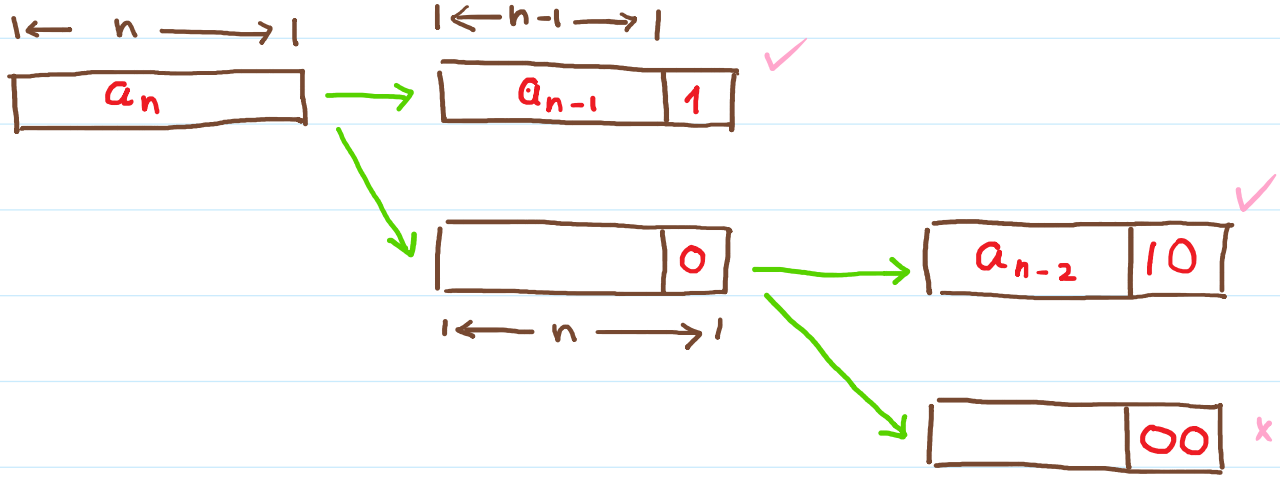
Let $a_n$ = # bacteria after n hours

$= 2a_{n-1}$ (double every hour)

Initially $a_0 = 5$. initial condition

Ex. Find the RR and give initial condition for # bit strings of length n that do not have two consecutive zeros.

Let $a_n$ = # bit strings of length n with no 00




$a_n = a_{n-1} + a_{n-2}$

We need 2 initial condition

$a_1 = 2, \quad a_2 = 3 \qquad \{10, 01, 11\}$

For $a_5 = ?$

$a_3 = a_2 + a_1 = 5$

$a_4 = a_3 + a_2 = 8$

$a_5 = a_4 + a_3 = 13$

patterns

~~0000~~ ~~1000~~
~~0001~~ ~~1001~~
~~0010~~ 1010 ✓
~~0011~~ 1011 ✓
~~0100~~ ~~1100~~
0101 ✓ 1101 ✓
0110 ✓ 1110 ✓
0111 ✓ 1111 ✓

## Solving Recurrence Relation

**Def.** Linear, homogenous RR of degree $k$ with constant coefficients is:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

$\exists \; c_i \in \mathbb{R}$ and $c_k \neq 0$