1/3/18

Using mathematical induction

Example: Prove that every amount of postage of 12 cents or more can be formed using just 4-cent & 5-cent stamps (Postage Stamp problem).

Basis: $n = 2$ can be generated using 3 4-cent stamps.

Inductive step: Let $P(k)$ be true, $k \geq 12$.

i.e. k cents can be formed using 4 cents & 5 cents stamps.

Case 1: at least one 4-cent stamp used to form postage of k cents.

Replace one 4-cent stamp by a 5-cent stamp.

Case 2: No 4-cent stamps were to form postage of k-cents as $k \geq 12$ at least three 5-cents stamps were used to generate postage of k cents.

Replace it by four 4-cent stamp

Proof using Strong induction

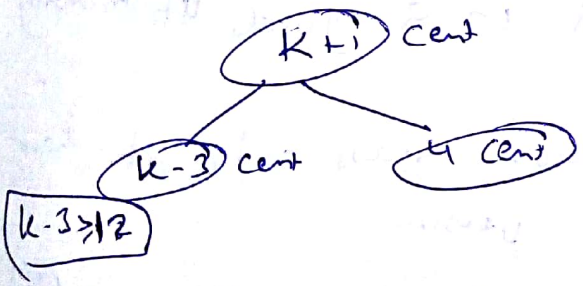
Base $12 = 4 \times 3$

$13 = 4 \times 2 + 5 \times 1$

$14 = 2 \times 5 + 1 \times 4$

$15 = 3 \times 5$

Inductive step: Let $P(j)$ be true for $12 \leq j \leq k$, where k is an integer ≥ 15



Example:- (Fundamental Theorem of Arithmetic / Unique factorization Theorem)

prove using well-ordering principle

Every +ve int $a>1$ can be uniquely expressed as the product of primes.

i.e. $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$; $\alpha_1, \alpha_2, \cdots \alpha_n \in \mathbb{N}$

$p_1 < p_2 < \cdots < p_n$

Proof:- Using (strong) induction (Existence).

Base $P(2)$ is true $P(n) =$ has unique factorization

Inductive step :- Let $P(2), P(3), \cdots P(k)$ be true.

Consider $P(k+1)$

→ Case 1 $k+1$ is prime. → done ($P(k+1)$ is true)

→ Case 2 $k+1$ is not prime.

↳ $k+1 = ab$; $1 \le a, b \le k$

by induction hyp. a, b have unique prime factorization.

Uniqueness Proof (by contradiction)

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$

$p_1 < p_2 < \cdots < p_n$; $q_1 < q_2 < \cdots < q_l$

↳ List are distinct

$p_1 \mid p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$

$\Rightarrow p_1 \mid q_j$ for some j, $1 \le j \le l$

$\hookrightarrow \leftarrow$

Example:- (odd pie fight)

→ An odd no. of people stand in a yard at mutually distinct distances.

→ At the same time each person throws a pie at their nearest neighbour, hitting this person.

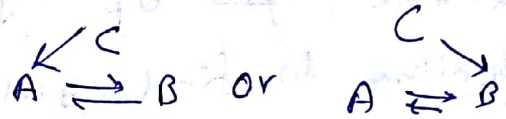
Sol^n :- Use mathematical induction to show that there is at least one survivor, that is, at least person who is not by a pie.

$P(n) \rightarrow$ there is a survivor whenever $2n+1$ people stand in a yard at distinct mutual distances & each person throws a pie at their nearest neighbour.

Proof

Base $P(1)$

$2 \times 1 + 1 = 3$ people



A, B nearest to each other
C is not hit.

Inductive step $P(k)$ true

Claim:- $P(k+1)$ is also true.

$P(k+1) \rightarrow 2(k+1)+1 \rightarrow 2k+3$ people.

Let A, B are the closest pairs among this group of $2k+3$ people.

Case I. Someone else throws a pie to either A or B
$A \rightleftarrows B$.
$2k$ pies to be thrown among $2k+1$ people

Case 2 no one else throws a pair at either A or B.

Besides A, B we have $2k+1$ people, $2k+1$ pies. By induction one survivor S.

5|3|B → **Lame's theorem :-**

Let a and b be positive integer with $a \geq b$ then the # of division used by Euclidean algorithm to find $\gcd(a,b) \leq 5 \times (\log_{10} b + 1)$.

Euclidean Algo :

Let $a = r_0$, $b = r_1$.

$r_0 = r_1 q_1 + r_2 \quad ; \quad 0 \leq r_2 < r_1$

$r_1 = r_2 q_2 + r_3 \quad ; \quad 0 \leq r_3 < r_2$

$r_2 = \quad , \quad$

$r_{n-2} = r_{n-1} q_{n-1} + r_n \quad ; \quad 0 \leq r_n < r_{n-1}$

$r_{n-1} = r_n q_n$

Division Algo.

If a, b are integers with $b \geq 1$, then $\exists$ unique integers q & r s.t.

$a = bq + r$ (q unique) $\quad 0 \leq r < b$.

Proof :- Exercise using well-ordering principle.

q → quotient ; r → remainder.

Quotients $q_1, q_2, \ldots, q_{n-1}, q_n \geq 1$ each

$q_n \geq 2$ i.e. $q_n \neq 1$

$f_0 = 0, \; f_1 = 1, \; f_2 = 1, \; f_3 = 2, \; f_4 = 3.$

$r_n \geq 1 = f_2.$

$r_{n-1} = r_n q_n \geq 2 r_n \geq 2 f_2 = f_3$

$r_{n-2} = r_{n-1} q_{n-1} + r_n \geq r_{n-1} + r_n \geq f_2 + f_3 = f_4.$

$r_2 \geq r_3 + r_4 \geq f_{n-1} + f_{n-2} = f_n$.

So, $b = r_1 \geq r_2 + r_3 \geq f_{n+1}$

Exercise

($f_n > \alpha^{n-2}$; when α = Golden ratio $= \frac{\sqrt{5}+1}{2}$)

So, $b = r_1 \geq r_2 + r_3 \geq f_{n+1} > \alpha^{n-1}$

$\log_{10} \alpha = \frac{1}{5}$

$\Rightarrow \log_{10} b \geq (n-1) \log_{10} \alpha$.

$\Rightarrow \log_{10} b \geq \frac{(n-1)}{5}$

$(n-1) < 5 \log_{10} b$

$\Rightarrow n < 1 + 5 \log_{10} b \Rightarrow n < 5k+1$; where k = # of digits in b.

$n \leq 5k = 5\lfloor \log_{10} b + 1 \rfloor \leq 5(\log_{10} b + 1)$.

Example:- Solve the System of Congruences.

$x = 2 \pmod 3$

$x = 3 \pmod 5$ by CRT $\rightarrow$ Soln

$x = 6 \pmod{14}$

$$x = \sum_{i=1}^{3} a_i m_i N_i \bmod N$$

$a_1 = 2, \ a_2 = 3, \ a_3 = 6$ $\quad N = n_1 n_2 n_3 = 210$.

$n_1 = 3, \ n_2 = 5, \ n_3 = 14$ $\quad N_1 = n_2 n_3 = 70$

$N_2 = n_1 n_3 = 42$

$N_3 = n_1 n_2 = 15$

for $x \bmod 3 = 1$

$m_1 = N_1^{-1} \bmod n_1 = 70^{-1} \bmod 3 = 1$

$m_2 = N_2^{-1} \bmod n_2 = 42^{-1} \bmod 5 = 3$

$m_3 = N_3^{-1} \bmod n_3 = 15^{-1} \bmod 14 = 1$

So, the CRT Soln mod 210 is

$x = 2 \times 1 \times 70 + 3 \times 3 \times 42 + 6 \times 1 \times 15$

$= 608 \bmod 210 = 188$.

To find modular Inverse

Extended Euclidean algo.

Input : $a, b, b \geq 1, a > b$

Output : $d = gcd(a,b)$; u, v integer s.t.

$d = au + bv$

Bezout's identity

Theorem:- Bezout's identity:-

Suppose that a & b are integers not both equal to zero & let $d = gcd(a,b)$

Then there exist integer x & y are showing that str. $\exists$

In the specific case in which a & b are relatively prime, we can write $= ax + by$

To find modular inverse

Extended Euclidean algm

Input :- $a, b, \quad b \geq 1, \quad a > b$

Output $d = gcd(a,b)$, u, v >)

$d = au + bv$

Bezout's identity.

$\bar{a}^{-1} \bmod b$.

$d = au + bv$.

$= \bar{a}v \bmod b = y$

$U(1) = a = a(1,2) + b\,U(3)$; $V(1) = b = a(V(2)) + bV(3)$

$= a.1 + b.0$ $= a.0 + b.1$.

Step 1 :- Set $U = [a, 1, 0]$, $V = [b, 0, 1]$

Step 2 :- while $(V(1) > 0)$.

$W = U - \left[\frac{U(1)}{V(1)}\right] V$.

Update $U = V$

Update $V = W$ end [while]

$v \mid u \mid q = \frac{u(1)}{v(1)}$

$w \mid v$

$u(1) = v(1)$ & $u(2) - w(1)$

$u(2) = v(2)$ & $u(3) - w(2)$

$u(3) = v(3)$ & $u(3) - w(3)$

Step 3:- Output.

$d = u(1)$

$u = u(2)$ Claim: $d = au + bv$.

$v = u(3)$

Example:- a) Compute $d = \gcd(148, 75)$ & integers u, v. s.t. $d = 148u + 75v$.

b) If exist compute $75^{-1} \bmod 148$.

$q = \frac{u(1)}{v(1)}$	$u(1)$ $u(2)$ $u(3)$	$v(1)$ $v(2)$ $v(3)$
	148 1 0	75 0 1
1	75 0 1	73 1 -1
1	73 1 -1	2 -1 2
36	2 -1 2	1 37 -73
2	1 37 -73	0 -75 149.
	y_d y_u y_v	

$d = \gcd(148, 75) = 1$.

$= 148 \times 37 + 75 \times -73$

a)

b) Take mod 148 in above

$75^{-1} \bmod 148 = -73$.

6/3/18

Structural Induction

Example :- (Rooted Binary tree)

Basic Step :- There is a full binary tree consisting of a single vertex r.

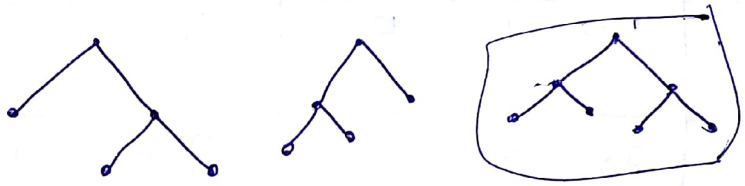
(Recursive Step):- If T_1 & T_2 are disjoint full binary trees there is a full binary tree T_1, T_2 consisting of r together with edges connecting root of the left subtree T_1 to r & root of right subtree T_2 to r.

T_1 T_2
$\hookrightarrow T_1, T_2$.

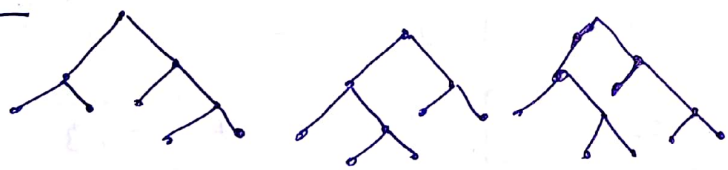
Basic Step :-

Step 1.

Step 2



Step 3



$h(T_1) \rightarrow$ height of T_1, $n(T_1)$ = # of nodes in T_1

$h(T_2) \rightarrow$ height of T_2, $n(T_2)$ = # of nodes in T_2.

Then $h(T) = \max(h(T_1) + h(T_2)) + 1$

$n(T) = n(T_1) + n(T_2) + 1$.

$$\leq 2^{h(T_1)} - 1 + 2^{h(T_2)} - 1 + 1$$

$$\leq 2 \times \max\{2^{h(T_1)+1}, 2^{h(T_2)+1}\} - 1$$

$$\leq 2 \cdot 2^{\max\{h(T_1)+1, h(T_2)+1\}} - 1$$

$$= 2 \cdot 2^{\max(h(T_1), h(T_2))+1} - 1 = 2 \cdot 2^{h(T)} - 1 = 2^{h(T)+1} - 1$$

Theorem :- Use structural induction to prove $n(T) \leq 2^{h(T)+1} - 1$

Proof :- (Base) T having only node r

$$n(T) = 1$$

$$h(T) = 0$$

$$2^{h(T)+1} = 2$$

$$n(T) = 1 < 2 = 2^{h(T)+1}$$

Inductive step :- $n(T_1) \leq 2^{h(T_1)+1} - 1$

$$n(T_2) \leq 2^{h(T_2)+1} - 1$$

when T_1, T_2 are full binary tree.

Generalization of induction

Can be extended over other sets having the well-ordering principle.

E.g. $N \times N$

Lexicographic ordering :-

(x_1, y_1) less than (x_2, y_2)

if $(x_1 < x_2)$ or $(x_1 = x_2 \text{ & } y_1 < y_2)$

Example :-

$(m, n) \in N \times N$.

define :- $a_{00} = 0$.

$$a_{m,n} = \begin{cases} a_{m-1,n} + 1 & \text{if } n = 0 \text{ \& } m > 0 \\ a_{m,n-1} + n & \text{if } n \neq 0 \end{cases}$$

→ Show that $a_{m,n} = m + \frac{(n)(n+1)}{2} \; \forall \; (m, n) \in N \times N$

Boolean Algebra

Boolean Expression in variable $x_1, x_2, \ldots x_n$.

Basic Step:- $0, 1, x_1, x_2, \ldots x_n$ are Boolean Algebra.

Recursive Step:- if $\mathcal{E}_1$ & $\mathcal{E}_2$ are Boolean ~~Algebra~~ Expression

then $\overline{\mathcal{E}_1}$, $\mathcal{E}_1\mathcal{E}_2$, $\mathcal{E}_1 + \mathcal{E}_2$ are Boolean Expression.

well-formed formulae for Compound Statement form

→ (T, F, propositional variables, and operators from the set $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$.

Recursively defined as:-

Basic Step:- T, F, S are well-formed formulae.

if E_1 & E_2 are well-formed formulae, then

$\neg E_1$, $E_1 \wedge E_2$, $E_1 \vee E_2$, $E_1 \rightarrow E_2$, $E_1 \leftrightarrow E_2$ are well-formed formulae.

The foundation of logic:- Propositional Calculus

- Propositional Variables / Statement Variables (p, q, r, s, ...)
- truth assignment (T, F)

Defn:- (Proposition)

→ a declarative statement that is either true or false, but not both.

Example :-

a) $4+5>3$

b) Napoleon is dead.

c) Are u Indian ?

d) $x+y=2$.

e) All signals are prognals.

Def^n (Paradox) → a statement that apparently contradicts itself & yet might be true.

Example :- Russel's paradox, $S = \{x | x \notin x\}$ → the set contain a set x iff x does not belong to itself.

Example: Liar's paradox.

p: This proposition is false.

Example :- (Pinocchio's paradox) 2010

Pinocchio is a wooden puppet who dream of one day becoming a real boy.

Pinocchio had such a nose when he tells a lie, his nose grows -

A paradox occur when pinocchio says

p :- "my nose is growing".

Exercise :- paradox or not?

" I know one thing : that I know nothing.

(Plato's proposition) -

Manipulating Symbol instead of words → Boole, Venn (1854)

Logical Connectives

i) $\neg p$ denote "not p"

ii) $p \wedge q$ denotes "p & q" (Conjunction)

iii) $p \vee q$ denote "p or q" (Disjunction)

iv) $p \dagger q = (p \vee q) \wedge \neg (p \wedge q)$

v) Implication (Conditional Statement)

$p \rightarrow q$ denotes "if p then q"

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

p is sufficient for q

q is necessary for p.

q, if p.

Example :- (falling in poision Ivy)

p = I fell in to poision Ivy.

q = I have a rash.

$p \rightarrow q$ would be

"If I fall into poision Ivy, then I will get a rash".

"q unless $\neg p$"

true if $\neg p$ is false.

↳ p is true.

antecedent or premise or hypothesis

Conclusion or Consequence.

Converse, Contrapositive, Inverse (derived from Logical implication)

- (Original) $p \to q$.
- Converse $q \to p$.
- (Contrapositive) $\neg q \to \neg p$. } equivalent
- Inverse $\neg p \to \neg q$.

$\neg q$	$\neg p$	$\neg q \to \neg p$
F	F	T
T	F	F
F	T	T
T	T	T

Example:- "If a man can march, then he is a soildier".
p q

↳ Contrapositive:-

Converse :-

Inverse :-

Example:- fermat's little theorem.

If n is a prime then $a^{n-1} \equiv 1 \pmod n$ when $gcd(a,n) = 1$
p q

Contrapositive :-

if $a^{n-1} \not\equiv 1 \pmod n$ when n is a +ve integer & $gcd(a,n) = 1$,
then n is not prime. (used for primality checking)

Input :- pick a witness $a < n$ with
$gcd(a,n) = 1$

Check if $a^{n-1} \not\equiv 1 \pmod n$.
then n is composite

Biconditional ($\leftrightarrow$)

$p \leftrightarrow q \rightarrow (p \rightarrow q) \wedge (q \rightarrow p)$

$p \leftrightarrow q$

"p if only if q"

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

nand $\uparrow$ $\neg(p \wedge q)$

nor $\downarrow$ $\neg(p \vee q)$

Order of precedence

$( ), \neg, \wedge, \vee, \rightarrow, \leftrightarrow$

Propositional equivalence

$(p \leftrightarrow q) \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$.

Tautology :- a proposition which is always true.

Example :- $(p \vee \neg p)$

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
T	F	T	F
F	T	T	F

Contradiction :- ~~It always false~~

It is always false under all possible truth assignment of the variable contained.

Example :- $p \wedge \neg p$

Contingency :-

$p \Leftrightarrow q$: not a connective → rather it is a statement that **$p \Leftrightarrow q$ is a tautology**

12/3/18

Rules of Inference

		Tautology	Name
1.	$p \to q$ p $\therefore q$	$(p \to q) \wedge p \to q$	Modus Ponens ↳ modes that affirm.
2.	$p \to q$ $\neg q$ $\therefore \neg p$	$(p \to q) \wedge \neg p \to \neg p$	Modus Tollens mode that denies

$\neg q \to \neg p$
$\neg q$
$\neg q$ by modus ponens

p	q	$(p \to q) \wedge p \to q$
T	T	T
T	F	T
F	T	T
F	F	T

Using resolution principle

$C_1 : \neg p \vee q$.

$C_2 : \neg q$.

$C_3 : \neg(\neg p) : p$.

$C_4 = q$.

3. $p \to q$
$q \to r$
$\therefore p \to r$

Tautology $([p \to q] \wedge [q \to r]) \to [p \to r]$

Name: Hypothetical Syllogism

4. $p \vee q$
$\neg p$
$\therefore q$

Disjunctive Syllogism

5. p
$\therefore p \vee q$

Addition.

(7) $C_1 = \neg p \vee q$
$C_2 = \neg q \vee r$
$C_3 = \neg(\neg p \vee r) = p \wedge \neg r$
$C_4 = p$
$C_5 = \neg r$
$C_6 = q$
$C_7 = r$

(9) $p \wedge q$
$\therefore p$

Simplification.

7. p
q
$\therefore p \wedge q$

Conjunction

8. $p \vee q$
$\neg p \vee r$
$\therefore q \vee r$

Resolution

Example:- "If you send me an email message, then I will finish writing program". $p \to q$

"If you not send me email message, then I will go to sleep early". $\neg p \to r$

"If I go to sleep early, then I will wake up feeling refreshed". $r \to s$

∴ "If I do not finish writing the program, then I will wake up feeling refreshed". $\neg p \to s$

Symbolic form:-

$p \to q$

$\neg p \to r$

$r \to s$

$\therefore \neg p \to s$

$\neg q \to \neg p$.

$\neg p \to r$

$\neg q \to r$ (Hypothetical syllogism)

$r \to s$

$\neg q \to s$ (By Hyp. syllogism)

Example:- (Quantified statements)

"Socrates is a man" Then $P(x)$ it is a man.

"All men are mortal" $m(x)$ it is mortal.

Conclusion "$P(\text{Socrates})$"

$\forall x (P(x) \to m(x))$.

$\therefore m(\text{Socrates})$ (why?)

$P(\text{Socrates})$

13/3/17

Fallacy :- A fallacy is an agreement that has an inherent flow in its structure that renders the argument invalid.

3 types of fallacies :-

(i) Affirming the Disjunction $\Rightarrow$ $\dfrac{p \vee q \quad p}{\therefore \neg q}$

(ii) Affirming the Consequence. $\Rightarrow$ $\dfrac{p \to q \quad q}{\therefore p}$

(iii) Denying the Antecedent $\Rightarrow$ $\dfrac{p \to q \quad \neg p}{\therefore \neg q}$

$\dfrac{p \to q \quad p}{\therefore q}$ modus ponens

Example :- (Political Syllogism)

If things are to improve, then things must change.
We are changing things.

Therefore, we are improving things.

Symbolic form

$\dfrac{i \to c \quad c}{\therefore i}$ invalid

$i \to$ things are improving
$C \to$ things changes

$C_1 : \neg i \vee c$
$C_2 : c$
$C_3 : \neg c$
$C_4 : \neg i$

$[(i \to c) \wedge c \to i] \hookrightarrow T$

Example:- (Denying the Antecedent)
(We cannot be machine turning)

If each man had a definite set of rules of Conduct by which he regulated his life, he would be no better than a machine.
But there no such rules. So, men cannot be machine.

Symbolic form:-

$r \rightarrow m$
$\neg r$
$\therefore \neg m$

$m \rightarrow$ man is machine
$r \rightarrow$ each man has a definite set of rules of conduct by which he regulated his life.

More Complex argument

Dilemma:- Dilemma is an argument in which both the hypothetical Syllogism & disjunction Syllogism are combined together.

Example:- (The paradox of Court)

- Ancient Greeks.
- Protagoras agreed to teach a Student named Euathlus in the art of Logic.
- The Condition being only half the fee is required at the time of instruction of the remaining fee due when Euathlus won his first case in Court.
- Should Euathlus fail, then the fee would be forfeited
- When Euathlus training was completed, he delayed to undertake any case.

- Eventually, Protagoras could not await longer for payment & decided to expedite the process.
- Protagoras decided to sue Euathlus.

Protagoras' Argument

1. If this case is decided in my favour, Euthalus must pay me by the order of the court.
2. If it is decided in Euthalus favour. Euthalus must pay me under the terms of the agreement.
3. But, it must be decided either in my favour, Or Euathlus favour.

Therefore, Euathlus is bound to pay me in any case.

Euthalu's Argument

1. If the case is decided in favour of protetoges, I am free by the term of the agreement.
2. If it is decided in my favour, I'm free by order of the court.
3. But, it must either be decided in protagora's favour Or my favor.

Therefore, I am discharge of my defeat in any case.

Predicates & Quantifiers

E.g. :- "x" is greater than 3"

P(x) a propositional f^n.

↳ when a value to x is assigned we set a proposition n-ary predicate → $P(x_1, x_2, x_3 \ldots x_n)$

Quantifier also used to set propositions

$\forall x\ P(x)$ (Domain should be specified).

$\exists$

Example:

(i) $P(x)$ = "$x+1 > x$" domain of discourse

$\forall x.\ P(x)$ is true → set of all real nos.

(ii) $Q(x)$ = "$x < 2$", domain consist of all real nos.

a) $\forall x\ Q(x)$ false as $Q(3)$ is false

b) $\exists\ Q(x)$ true as $Q(1)$ is true.

Example: $P(x)$ = "$x^2 \geq 10$"

domain → the integers not exceeding 4.

a) $\forall x P(x)$ means $P(1) \wedge P(2) \wedge P(3) \wedge P(4)$

b) $\exists x\ P(x)$ mean $P(1) \vee P(2) \vee P(3) \vee P(4)$.

Quantifiers with restricted domain

(i) $\forall x < 0\ (x^2 > 0)$, domain : Real nos

(ii) "The square of $-ve$ real no is positive".

$\forall x\ (x < 0 \rightarrow x^2 > 0)$

(iii) $\exists z > 0\ (z^2 = 2)$, domain = Real nos.

"There is a +ve square root of 2".

$\exists z\ (z > 0 \wedge z^2 = 2)$

Example:- (Lewis Carrol).

"All lions are fierce".

"Some lions do not drink Coffee".

"Some fierce creatures do not drink Coffee".

$\forall x (P(x) \rightarrow Q(x))$

$\exists x (P(x) \wedge \neg R(x))$ → Cannot be $P(x) \rightarrow \neg R(x)$.

$\exists x (Q(x) \wedge \neg R(x))$

Using one-way predicate, convert this to symbolic form

Domain → all creatures

$P(x)$ = x is a lion

$Q(x)$ = x is fierce

$R(x)$ = x drinks Coffee

for a specific x,

$P(x)$	$\neg R(x)$	$P(x) \rightarrow \neg R(x)$
T	F	F
T	F	F
F	T	T
F	F	T

$P(x) \rightarrow \neg R(x)$ is true even when $P(x)$ is false.

Example:- "All humming birds are richly colored".

"No large birds live on honey".

"Birds that do not live on honey are dull in color".

"Therefore, Humming birds are small".

Domain :- All birds

$P(x)$ = x is a hamming bird.

$Q(x)$ = x is large.

$R(x)$ = x lives on honey.

$S(x)$ = x is richly colored.

$\forall x (P(x) \rightarrow S(x))$

~~$\forall x (Q(x))$~~ $\neg \exists x (Q(x) \wedge R(x))$

$\forall x (\neg R(x) \rightarrow \neg S(x))$

$\therefore \forall x (P(x) \rightarrow \neg Q(x))$.

Check the validity of the argument using

(i) Rules of inference

(ii) Resolution Principle.

Example :- $\lim_{x \to a} f(x) \neq L$

- $\forall x P(x) \vee Q(x)$ mean $(\forall x P(x)) \vee Q(x)$
  - ↳ high precedence than $\vee, \wedge$, etc.
  - $\forall, \exists \rightarrow$
- $\forall x (P(x) \wedge Q(x)) \Leftrightarrow \forall x P(x) \wedge \forall x Q(x)$
  - $\vee$ ×
  - $\exists x (P(x) \vee Q(x)) \Leftrightarrow \exists x P(x) \vee \exists x Q(x)$.

Demorgen's Law

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

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

(Proof as exercise)

Example:- $\lim_{x \to a} f(x) \neq L$ — (1)

Use quantifiers & predicates to express (1).

$\lim_{x \to a} f(x) = L$ means

$\forall \varepsilon > 0 \; \exists \delta > 0, \forall x \; (0 < |x-a| < \delta \rightarrow |f(x) - L| < \varepsilon)$

↳ Poke negation

$\exists \varepsilon > 0 \; \forall \delta > 0, \exists x \; (0 < |x-a| < \delta \wedge |f(x) - L| \geq \varepsilon)$

$p \rightarrow q \iff \neg p \vee q$

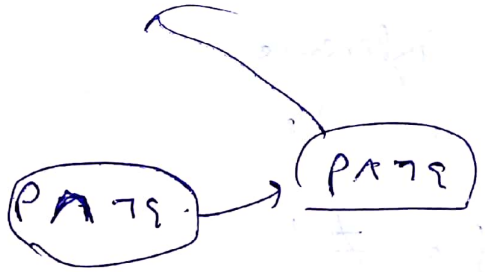
$\neg(p \rightarrow q) \iff p \wedge \neg q$

$\neg(a \rightarrow b) \iff a \wedge \neg b$

Proof.

$\neg(\neg a \vee b)$

$\neg\neg a \wedge \neg b \iff a \wedge \neg b$



Example:-

1) There is a no. n s.t. $n^2 = 441$. true eg $n = 21$

2) There are +ve integer a, b, c, d s.t.

$a^4 + b^4 + c^4 = d^4$

$2,682,440^4 + 15,365,639^4 + 18,796,760^4 = 20,615,673^4$

$x^n + y^n = z^n$, x, y, z +ve int

$n > 2$

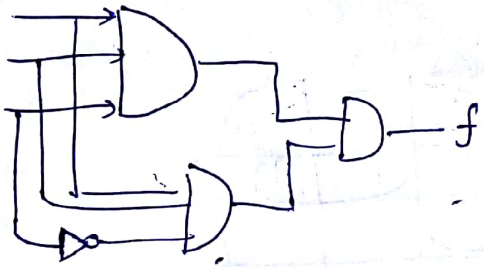
Fermat's last theorem

$\forall x \in X$, $x^2 + x + 41$ is a prime

20/9/18

Minimization of Combinational Circuit

Example :- $f = xyz + x\bar{y}\bar{z}$



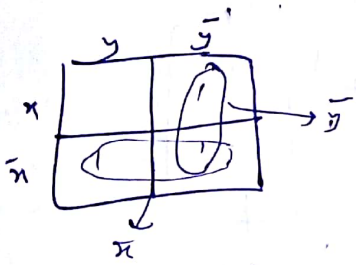
Two methods :-

1) Karnaugh's map (upto 6 variables)
2) Quine - mac Cluskey's method (upto 10 variables)

K-map

2 variables (x, y)

$2^2 = 4$

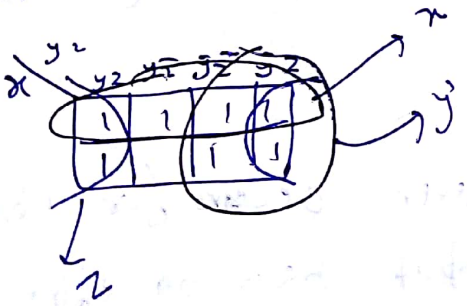


$f = x\bar{y} + \bar{x}y + \bar{x}\bar{y}$

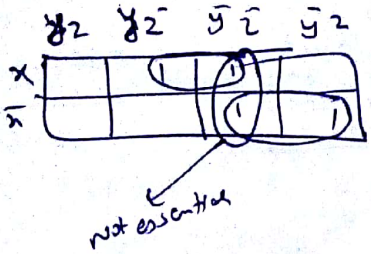
3 - variables ($2^3 = 8$)

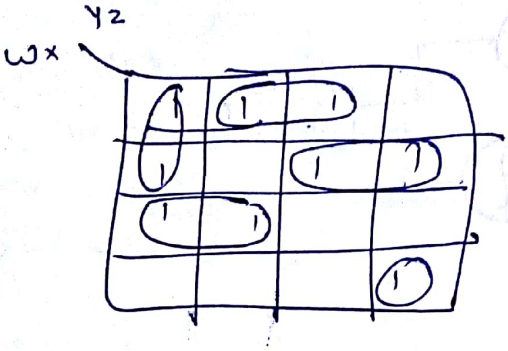
$f = xyz + xy\bar{z} + x\bar{y}z + x\bar{y}\bar{z} + \bar{x}yz + \bar{x}\bar{y}z + \bar{x}\bar{y}\bar{z}$

Simplify



$f = x + y + z$

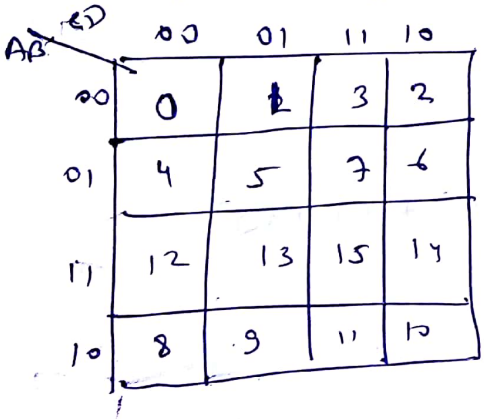


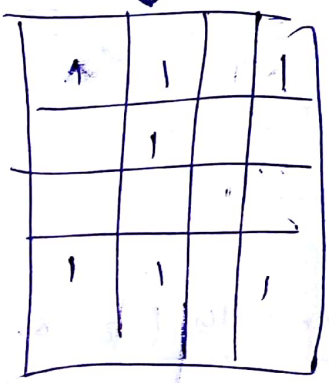


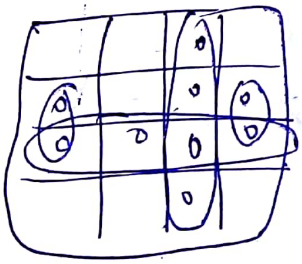
Example:-

$F(A,B,C,D) = \sum(0,1,2,5,8,9,10) = \bar{B}\bar{D} + \bar{B}\bar{C} + \bar{A}\bar{C}D$

Find the product of sum of F in most simplified form.







$\bar{F}(ABCD) = CD + AB + B\bar{D}$

$F = (\bar{F}) = (\bar{C}+\bar{D})(\bar{A}+\bar{B})(\bar{B}+D)$

Don't Care cdtn:-

- Some input combination never occurs for certain Circuits. these input have no effect on output.

Example :- BCD (Binary Circuit Decimal).

0, 1, 2, - - - 9.

→ 4 bit = 16.
2^4 →

Digit	BCD Codeword
0	0 0 0 0
1	0 0 0 1
2	0 0 1 0
3	0 0 1 1
4	0 1 0 0
5	0 1 0 1
6	0 1 1 0
7	0 1 1 1
8	1 0 0 0
9	1 0 0 1
	w x y z

Q) Suppose that a circuit to be built that produces an output { 1 if the decimal digit is ≥ 5; 0 if the decimal digit is < 5.

$F(wxyz) = \bar{w}x\bar{y}z + \bar{w}xy\bar{z} + \dots$

	yz	$y\bar{z}$	$\bar{y}\bar{z}$	$\bar{y}z$
wx	d	d	d	d
$w\bar{x}$	d	d	1	1
$\bar{w}\bar{x}$				
$\bar{w}x$	1	1		1

$F = w\bar{x}\bar{y} + \bar{w}xy + \bar{w}xz$

$F = w\bar{x} + \bar{w}xy + xyz.$

$= w + xy + xz$

Exercise:

$f(w,x,y,z) = \Sigma(1,3,7,11,13)$

Quine - Mccluskey Method

Example: Find the minimal expression equivalent to

$xyz + x\bar{y}z + \bar{x}yz + \bar{x}\bar{y}z + \bar{x}\bar{y}\bar{z}$.

Finding prime implicants

	minterms	bit string	# of 1's	Term	bit string
1.	xyz	111	3 (1,2)	xz	1-1 ✓ (1,3)
2.	$x\bar{y}z$	101	2 (1,3)	yz	-11 * (2,3)
3.	$\bar{x}yz$	011	2 (2,4)	$\bar{y}z$	-01 *
4.	$\bar{x}\bar{y}z$	001	1 (3,4)	$\bar{x}z$	0-1 ✓
5.	$\bar{x}\bar{y}\bar{z}$	000	0 (4,5)	$\bar{x}\bar{y}$	00-

(1,2,3,4)	z

Prime implicants :- $z, \bar{x}, \bar{y}$.

Cover finding table

	xyz	$x\bar{y}z$	$\bar{x}yz$	$\bar{x}\bar{y}z$	$x\bar{y}\bar{z}$
z	×	×	×	×	
$\bar{x}\bar{y}$				×	×

22/3/18

Quine-McClustay

- Identify the prime implicants
- find essential prime implicants & a cover.

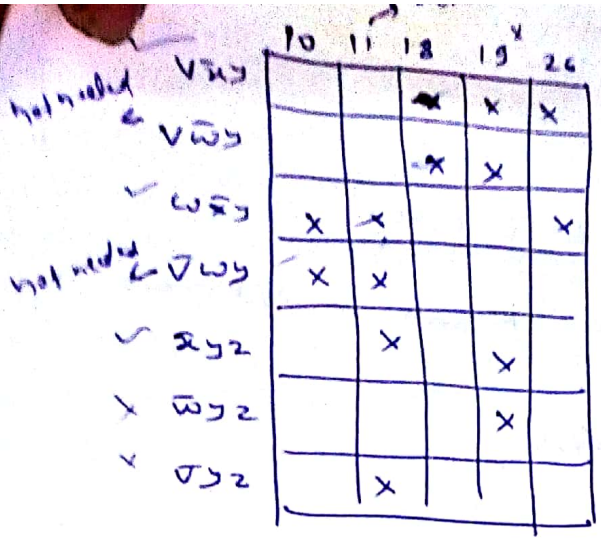
↳ Construct a table with prime implicants in each row & min. term in each column.

find a reduced chart by marking.

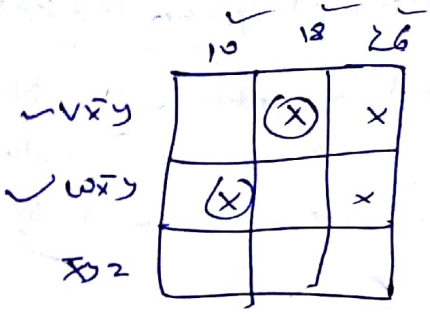
Example: $f(V,W,X,Y,Z) = \sum(1, 3, 4, 5, 6, 7, 10, 11, 12, 13, 14, 15, 18, 19, 20, 21, 22, 23, 25, 26, 27)$

Single cross column

	1	3	4	5	6	7	10	11	12	13	14	15	18	19	20	21	22	23	25	26	27
$\bar{W}X$			X	X	X	X			⊗	⊗	X	X			⊗	⊗	X	X			
$\bar{V}X$			X	X	X	X			⊗	⊗	X	X								X	X
$V\bar{X}$													X	X			X	X			
$V\bar{W}\bar{Y}$													X	X						X	X
$W\bar{X}Y$							X	X													
$\bar{V}WY$							X	X			X	X									
$\bar{X}YZ$	⊗	X						X					\	X							X
$\bar{W}YZ$		X				X												X			
$\bar{V}YZ$		X				X															
[illegible]																					
$\bar{V}\bar{W}Z$	⊗	X		X		X													⊗		⊗
$VW\bar{X}Z$																					



delete dominated rows.
delete dominating column.



$$f = \bar{w}x + \bar{v}x + \bar{v}\bar{w}x + vw\bar{x}z + vx\bar{y} + wx\bar{y}$$

Algebric Structures

- Groupoid :→ Closure — $a, b \in G \;\forall\; a, b \in G$
- Semigroup :→ Closure + associativity → $a*(b*c) = (a*b)*c$
- Monoid → Closure + associativity + existence of identity element — $\exists\, e \in G$ s.t. $a*e = e*a = a$
- Group → Closure + associativity + existence of identity + inverse of each element. — For each $a \in G$, $\exists$ an element $a^{-1} \in G$ s.t. $a*a^{-1} = a^{-1}*a = e$
- Abelian Group → Commutative group.

Examples:- $(Z, \cdot)$ → not group (as $2^{-1} \notin Z$)
↳ monoid with identity 1

Example2:- $M_2(R)$ → all 2×2 matrices over R +
- (addition) Group ? ↳ yes
- multiplication Group ? no

Example:- $Z_n = \{[0], [1], [2] \dots [n-1]\}$.

Abelian ✓

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$[1] + [2] = 0 = e$
$[2] + [1]$

Z_3

•	[0]	[1]	[2]
[0]	0	0	0
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

$[a][b] = [ab]$

$[a]+[b] = [a+b]$

[1] is identity.

26/3/18

Group

$(G, \circ)$ → binary Composition

a non-empty set.

i) Closure $a \circ b \in G \ \forall a, b \in G$

ii) Associative $a \circ (b \circ c) = (a \circ b) \circ c \ \forall a, b, c \in G$.

iii) identity $a \circ e = e \circ a = a$

iv) inverse of each element

$a \circ a^{-1} = a^{-1} \circ a = e$.

inverse of $a \in G \rightarrow a^{-1} \in G$.

Some properties of Group:-

1) e is unique → if not, let e, e' be two identity element of G.

$a \circ e = e \circ a = a$

$a \circ e' = e' \circ a = a$ → holds for e' also. $\forall a \in G$

$e' \circ e = e \circ e' = e'$

$e \circ e' = e' \circ e = e$

2) a^{-1} is unique

If not, let $b, c \in G$ be two inverse of a.

$a \circ b = b \circ a = e$

$a \circ c = c \circ a = e$

$c \circ (a \circ b) = c \circ e = c$

$(c \circ a) \circ b$

$e \circ b$

$b = c$

Example:- $(Z, \circ)$: $a \circ b = a + b - ab \ \forall a, b \in Z$.

Check whether $(Z, \circ)$ is a i) groupoid ✓

ii) Semigroup ✓

iii) monoid ✓

iv) Group ✗

3) $a \circ x = b$, $y \circ a = b$ } have unique soln in G.

$a, b \in G$

$x = a^{-1} \circ b$

x_1, x_2 two soln

$a \circ x_1 = b = a \circ x_2$

$a^{-1} \circ (a \circ x_1) = a^{-1} \circ (a \circ x_2)$

$\Rightarrow (a^{-1} \circ a) \circ x_1 = (a^{-1} \circ a) \circ x_2$

$\Rightarrow e \circ x_1 = e \circ x_2$

$\Rightarrow x_1 = x_2$.

4) Cancellation laws holds

- $a \circ b = a \circ c \Rightarrow b = c$.
  $\forall a, b, c \in G$.
- $a \circ b = c \circ b \Rightarrow a = c$
  $\forall a, b, c \in G$

5) $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ (try)

- $M_2(R) \rightarrow$ Set of 2×2 matrices over R
  multiplication $\rightarrow$ not a group.
- $GL(2, R) \rightarrow$ general linear group (under matrix multiplication) of degree 2 on R
  (all $2 \times n$ non-singular matrices)
- $GL(n, R) \rightarrow$ general lin. gr. of degree n over R.

Theorem:- $(G, \cdot)$ Semigroup where each of the eqn $a \circ x = b$ & $y \circ a = b$ has a soln in G.
$\Rightarrow (G, \circ)$ is a group.

Proof:- $(G, \circ)$ Semigroup $\Rightarrow$ Closure, associativity hold

Existence of identity:-

Let e be a soln of $a \circ x = a$ $\Rightarrow a \circ e = a$ — (1)

& e' be a soln of $y \circ a = a$ $\Rightarrow e' \circ a = a$ — (2)

Let $c \in G$ be any element.

Consider the eqtn $a \circ x = c \longrightarrow b$ be a soln of this.
$y \circ a = c \longrightarrow q$ be a soln of this

$a \circ b = c$ — (3)
$q \circ a = c$ — (4)

$c \circ e = (q \circ a) \circ e$ by (4)
$= q \circ (a \circ e)$
$= (q \circ c)$ by (1)
$= c$ by (4)

As $c \in G$ arb., we have

$a \circ c = a \ \forall \ a \in G$ — (A)

$e' \circ c = e' \circ (a \circ b)$ by (3)
$= (e' \circ a) \circ b = a \circ b$ by (3)
$= c$ by (3)

As $c \in G$ arb, we have

$e' \circ a = a \ \forall \ a \in G$ — (B)

(A) holds for $a = e'$ also.

$e' \circ e = e' \longrightarrow e' = e$
(B) holds for $a = e$ also
$e' \circ e = e$

Inverse of each element $a \in G$

↳ Consider the eqtn.

$a \circ x = e \longrightarrow a' \in G$ be the soln.

$a \circ a' = e \longrightarrow a'' \circ (a \circ a') = a'' \circ e = a''$

$a'' \circ a = e$. ⇓

$(a'' \circ a) \circ a' = e \circ a' = a'$

Exercise :- Let (G, o) be a semigroup containing finite no. of elements where both the cancellation laws hold. Then prove that (G, o) is a group. (Use the previous theorem).

Exercise :- Let (G, o) be a finite semigroup & $a \in G$

(iv) Prove that $\exists$ +ve integers m, n s.t.

$$a^{mn} = a^m$$

v) Deduce that a^{mn} is an idempotent element in the semigroup

↓

Prove that $a^{mn} \circ a^{mn} = a^{mn}$.

Example:- Let (G, o) be a group, $a \in G$.

Define a mapping $f_a : G \to G$ by

$$f_a(x) = x \circ a, \quad x \in G$$

Show that f_a is a bijection.

One to one ?

$f_a(x_1) = x_1 \circ a$ $\quad f_a(x_1) = f_a(x_2)$

$f_a(x_2) = x_2 \circ a \Rightarrow x_1 \circ a = x_2 \circ a$

$\Rightarrow x_1 = x_2$ by right cancellation law.

Soln of this.

as (G, o) is group soln of this.

Onto :-

Let b be any arb- element in the co-domain set G.

$b \in G$, $a \in G \Rightarrow \exists$ a unique soln of the eqtn

$y \circ a = b$.

This y is the preimage of b.

Exercise: Let $(S, \circ)$ be a Semigroup. If for $x, y \in S$, $x^2 \circ y = y = y \circ x^2$, prove that $(S, \circ)$ is abelian group. Commutative.

27/03/17

Order of an element in a group

- (G, o) → a group
- $a \in G$
- $o(a)$: order of a = least +ve integer n s.t $a^n = e$

Order of a group G. $O(G)$ = # of elements in G.

Example :- $G = \{1, \omega, \omega^2\}$: $\omega^3 = 1$

$(G, \cdot)$

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	ω	1

abelian.

$O(G) = 3$

$O(1) = 1$

$O(\omega) = 3$

$O(\omega^2) = 3$.

Example : (V klein's 4 group).

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$a \cdot a = e \Rightarrow a^{-1} = a$

$b \cdot b = e \Rightarrow b^{-1} = b$

$c \cdot c = e \Rightarrow c^{-1} = c$

$e \cdot e = e \Rightarrow e^{-1} = e$

$O(e) = 1$

$O(a) = 2$ $\quad a^2 = e \Rightarrow a^{-1} = a$

$O(b) = 2$

$O(c) = 2$

Example :-

$(Z_n, \cdot)$ not a group

$(Z_n - [0], \cdot)$ is a group when n is a prime.

set of all units $Z_n^* = \{ a \in Z_n \mid \gcd(a, n) = 1 \}$.

Yes $(Z_n^*, \cdot)$ is a group $\{[0], [1], \ldots [n-1]\} \Rightarrow a \cdot x \equiv 1 \bmod n$,

$a^{-1} \bmod n = x \in Z_n$

$Z_8^* = \{[1], [3], [5], [7]\}$

$Z_8 = \{[0], [1], [2], \ldots [7]\}$.

$\overset{\to 1}{\cdot}$	$[1]$	$\overset{\to 2}{[3]}$	$\overset{\to 2}{[5]}$	$[7]$
$[1]$	$[1]$	$[3]$	$[5]$	$[7]$
$[3]$	$[3]$	$[1]$	$[7]$	$[5]$
$[5]$	$[5]$			
$[7]$	$[7]$			

→ forms a null group.

Theorem:- $a \in G$; $(G, \cdot)$ a group.

(i) $O(G) = O(G^{-1})$

(ii) $O(a) = n$ & $a^m = e \Rightarrow n \mid m$.

(iii) $O(a) = n \Rightarrow a, a^2, a^3, \ldots (a^n = e)$ are distinct elements of G. i.e. $O(a) \leq O(G)$.

(iv) (Order of power formula)

$$O(a^r) = \frac{O(a)}{\gcd(r, O(a))} \quad \text{i.e.} \quad \boxed{O(a) = n \Rightarrow O(a^r) = \frac{n}{\gcd(r, n)}}$$

(v) $O(a) = n \Rightarrow O(a^b) = n$ iff b is coprime to n.

(vi) $O(a)$ infinite & b is any +ve integer $\Rightarrow O(a^b)$ is infinite.

Proof:- (i) Let $O(a) = n$

$\Rightarrow a^n = e$, n is least such +ve integer.

$(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$.

if possible, let $\exists\ m < n$ s.t. $(a^{-1})^m = e$.

i.e. $a^m = e$.

$a^{-m} \in a$, $a^n \in G \Rightarrow a^{n-m} \in G$ s.t. $a^{n-m} = e$ (when $n-m < n$) ($\hookrightarrow \leftarrow$) as $o(a) = n$.

$\Downarrow$

$a^n = e$, n least $a^n \cdot a^{-m} = e \cdot e = e$

ii) as $o(a) = n$ & $a^m = e \Rightarrow m > n$

By division algo,

$m = nq + r$, $0 \le r < n$

$e = a^m = (a^n)^q a^r$

$= 1^q a^r = a^r$.

$\Rightarrow r = 0$

$\therefore m = nq$

$a^3 = e$; $a^6 = e$; $a^9 = e$; $a^{12} = e$

Application :-

Example :- $(G, \circ)$ group.

- $a \in G$ with $o(a) = 30$
- $\therefore o(a^{18}) = ?$

$$o(a^{18}) = \frac{o(a)}{\gcd(18, o(a))} = \frac{30}{\gcd(18,30)} = \frac{30}{6} = 5.$$

Example :- Find all elements of order 8 in the group $(Z_{24}, +)$.

$Z_{24} = \{[0], [1], [2], \ldots [23]\}$

if $o([1]) = l$, then $l[1] = [0]$, (l is least +ve integer)

$o([1]) = 24$ $\qquad$ $l = 24$

$o([m]) = 8$

$\downarrow$

$m[1]$.

$$8 = o([m]) = o(m[1]) = \frac{o[1]}{\gcd(m, o[1])} = \frac{24}{\gcd(m,24)}$$

$\gcd(m, 24) = \frac{24}{8} = 3$.

$m = 3, 6, 9, 12, 15, 18, 21$

$\times \quad \times \quad \times$

$[3], [9], [15], [21]$ order 8.

Proof iii) $a^i = a^j$; $i \ne j$, $i > j$.

$\Rightarrow a^{(i-j)} = e$ $\quad 0 \le i, j \le n$.

$i - j < n$ ($\hookrightarrow \leftarrow$) as $o(a) = n$.

v) $o(a^b) = \frac{o(a)}{\gcd(b, o(a))} = o(a)$ if $\gcd(b, n) = 1$.

Proof (v) To prove $o(a^m) = \frac{o(a)}{\gcd(m, o(a))}$.

(let $o(a) = n$ & $o(a^m) = k$.) $\Rightarrow$ n is least +ve integer s.t. $a^n = e$.

k is least +ve integer s.t. $(a^m)^k = e$

$a^{mk} = e$

$n \mid mk$; using (ii)

$\Downarrow$ value of k i.e. $v \mid k$ $\Rightarrow$ $v \mid k$ as $\gcd(u, v) = 1$

(let $d = \gcd(m, n)$

$u = \frac{m}{d}$, $v = \frac{n}{d}$ $\Rightarrow$ $m = ud$, $n = vd$

$\Rightarrow 1 = \gcd\left(\frac{m}{d}, \frac{n}{d}\right)$.

$\Downarrow \quad \Downarrow$

$u \quad v$ (i.e. $\gcd(u, v) = 1$)

Claim:- $V = k = \frac{n}{d} = \frac{o(a)}{\gcd(m, o(a))}$

Example:- $(G, \circ) \Rightarrow$ a group,
$a, b \in G$ commutes &
$o(a)$, $o(b)$ are coprime.
Then prove that $o(a \circ b) = o(a) \circ o(b)$.

Consider $(a^m)^k = (a^{dq})^k$
$= (a^n)^q = e^q = e$

As $o(a^m) = k$.
k is least +ve integer satisfying $(a^m)^k = e$.
$\Rightarrow k \mid n$ by (ii)

Sol^n:- Let $o(a) = n$
$o(b) = m$.
$o(a \circ b) = k$

$\gcd(m, n) = 1$
$a^n = e$, n least such +ve int
$b^m = e$, m " "
$(a \circ b)^k = e$, k " "

$a \circ b = b \circ a$

Claim: $(a \circ b)^t = a^t \circ b^t$ $\forall$ +ve integer t.

$(a \circ b)^2 = (a \circ b) \circ (a \circ b) = a \circ (b \circ a) \circ b = a \circ (a \circ b) \circ b$
$= a^2 \circ b^2$

$a^k \circ b^k = e$
$\Rightarrow a^k = b^{-k}$
$\Rightarrow a^{kn} = b^{-kn} = e \Rightarrow m \mid kn$ as $o(b) = m$
$\Rightarrow m \mid k$ as $\gcd(m, n) = 1$ — (1)

Similarly, $a^k = b^{-k} \Rightarrow a^{km} = b^{-km} = e$
$\Rightarrow n \mid km$
$\Rightarrow n \mid k$ as $\gcd(m, n) = 1$ — (2)

(1), (2) $\Rightarrow mn \mid k$ as $\gcd(m, n) = 1$. — (3)

Also $(a \circ b)^{mn} = a^{mn} \circ b^{mn} = e^m \circ e^n = e$.
As $o(a \circ b) = k$, we must have $k \mid mn$ — (4)

(3), (4) $\Rightarrow mn = k$ — $o(a \circ b)$
$= o(a) \, o(b)$

Example:- $(G, \circ)$ group of even order. Then prove that G contains an odd no. of element having order 2.

Sol^n $a \in G$: $o(a) = o(a^{-1})$

Case:1 $o(a) < 3$ $\quad o(a) = 1$ or 2
$\Rightarrow a = e$ $\quad a^2 = e$, 2 least +ve int.
$\Rightarrow a^{-1} = a$.

Case:2 $o(a) \geq 3$

2/4/18

Permutation group

$n! \to 2n$ permutation
$3! = 3 \times 2 = 6$.

- Symmetric group of degree n (S_n) → dihedral graph (D_n)

$S = \{1, 2, \ldots, n\}$ → Set of all permutation of S. → G, $|G| = n!$

(having sym of equilateral triangle / of an)

$$f = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ f(1) & f(2) & \ldots & & f(n) \end{pmatrix}$$

$f: S \to S$ a bijection

Then $(G, \cdot)$ forms a non-commutative graph for $n \geq 3$.

$$f \cdot g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

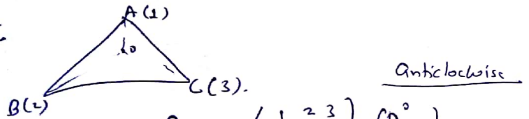
$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix} ; \quad g = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ f(1) & f(2) & \ldots & & f(n) \end{pmatrix}$$

Then

$$f \cdot g = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(g(1)) & & \ldots & f(g(n)) \end{pmatrix}$$

↓ exactly same as the set $\{1, 2, \ldots, n\}$ in same order.

S_3



Anticlockwise

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad (0°)$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad (60°)$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad (120°)$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad (\text{reflection about } AO)$$

$$\rho_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad (\text{" " } BO)$$

$$\rho_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad (\text{" " } CO).$$

Symmetry :- a symmetry of a geometrical figure in a Euclidean space is an isometry that keeps the figure as a whole unchanged.

- Euclidean space → a line – 1-space, a plane – 2-space.
- isometry → bijection from S to S that preserves distance between the points in S.

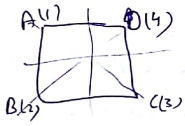
(S → Set of all pts. in a Euclidean space).

$\rho_2 \rho_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \rho_5$. | $\rho_1 \rho_3 \neq \rho_3 \rho_1$

$\rho_4 \rho_2 =$

$2 \times 4 = 8$ Symmetry.

S_4



$\rho_0 =$ 0° dihedral graph D_4.
$\rho_1 =$ 90
$\rho_2 =$ 180
$\rho_3 =$ 270

$\rho_4 =$ reflection about OH
$\rho_5 =$ " OV.
$\rho_6 =$ " AC
$\rho_7 =$ " BD

Example:- (Alternating group of order n) → A_n, $n \geq 1$.

→ • the set of all even permutation on the set $\{1, 2, \ldots n\}$
• sym. gp. of permutation forms, group

Can be decomposed into even no of transposition

Y-Cycle

$= (a_1, a_2 \ldots a_y)$

$= (a_1 a_y)(a_1 a_{y-1}) \ldots (a_1 a_2)$

2 cycle - transposition.

1 cycle.

$(a_r) = (a_r a_s)(a_r a_s)$

$f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$= (1)(2)(3)$

$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (2\ 3\ 1) = (2,1)(3,1)$

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$= (3\ 1\ 2)$

$D_5 \rightarrow 2 \times 5 \Rightarrow 10$ symmetries.

Order of permutation

- Let f be a permutation on a finite set s.
- order of f → smallest +ve integer n s.t. $f^n = i$, i being the identity permutation.

$i = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$

Theorem:- The order of a permutation on a finite set is the lcm of the length of its disjoint cycles.

$f^2 f^3 = f^3 f^2 = i = f^5$

$f f^{n-1} = i = f^{n-1} f$

$(f^3)^{-1} = f^2$

decomposition of a permutation

$a_r = (a_r a_s)(a_r a_s)(a_r a_m)(a_r a_m) \ldots$

Theorem: s finite set

# of even permutation on s = # of all permutation in s (check for s_3 or s_4)

even { • odd × odd → • even × even →

odd { • even × odd → • odd × even →

- inverse of an even permutation → even
- inverse of an odd permutation → odd

$\rho = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (1)(4,2)$

Order of ρ → 2

$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (2,3,1)$

Order of $\beta = 3$.

3/4/2012

Cyclic group :- $(G, \circ)$ cyclic if $\exists$ an element $a \in G$ s.t. $G = \{a^n \mid n \in \mathbb{Z}\}$

$G = \langle a \rangle$

↳ multiplicative group.

For additive gr :

$G = \langle a \rangle = \{na \mid n \in \mathbb{Z}\}$

Example :- (i) $(\mathbb{Z}, +)$ generated by 1 & -1 — infinite cyclic group.

$\mathbb{Z} = \langle 1 \rangle$

also $\mathbb{Z} = \langle -1 \rangle$.

(ii) $(\mathbb{Z}_4, +)$ cyclic generated by $[1], [3]$

(iii) V-Klein's 4 group → not cyclic

(iv) $S = \{1, i, -1, -i\}$, multiplication

→ generators i & $-i$

→ So cyclic.

Theorem :- If $G = \langle a \rangle$, then a^{-1} is another generator of G.

$G = \{a^n \mid n \in \mathbb{Z}\}$.

$b \in G \Leftrightarrow b = a^r$ for some $r \in \mathbb{Z}$

$\Leftrightarrow b = (a^{-1})^r$; $r \in \mathbb{Z}$.

Theorem Every cyclic group is abelian (Converse not true) Eg. V-Klin's 4 group abelian, but not cyclic.

$G = \langle a \rangle$

$b = a^{r_1}$

$c = a^{r_2}$; $r_1, r_2 \in \mathbb{Z}$

$b \circ c = a^{r_1} \circ a^{r_2} = a^{r_1 + r_2} = a^{r_2 + r_1} = a^{r_2} \circ a^{r_1}$

$= c \circ b$.

not abelian ⇒ not cyclic

Eg D_4 not abelian, so not cyclic.

S_3 not abelian, so not cyclic.

Theorem :- A finite group $(G, \circ)$ is cyclic of order n iff $\exists$ an element $a \in G$ st $o(a) = o(G) = n$.

Proof :- Let $(G, \circ)$ be a cyclic group of order n.

let $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Claim $o(a) = n$

let $o(a) = k$

Then $\{a, a^2, \ldots, a^k\} \subseteq G$ — (1)

let $b \in G$

So, $b = a^m$ for some $m \in \mathbb{Z}$

By division algorithm $m = kq + r$; $0 \le r < k$

$\therefore b = a^{kq+r} = (a^k)^q \circ a^r = a^r \in \{a, a^2, \ldots, a^k\}$.

$\therefore G \subseteq \{a, a^2, \ldots, a^k\}$ — (2)

(1), (2) ⇒ $G = \{a, a^2, \ldots, a^k\}$

$k = o(G) = n = o(a)$

Note :- if G is a finite cyclic gr. generated a then $G = \{a, a^2, \ldots, (a^n = e)\}$

Conversely, Let $\exists$ an element $a \in G$ s.t. $o(a) = n = o(G)$ when G is a finite gr.

Claim G is cyclic i.e. $G = \{a^i \mid i \in \mathbb{Z}\}$

Proof:- As $O(a) = n$, we have

$a, a^2, \ldots (a^n = e)$ are distinct elements of G.

Also $O(G) = n$

$G = \{a, a^2, \ldots a^n\} \subseteq \{a^i \mid i \in \mathbb{Z}\}$

$a \in G \Rightarrow \{a^0, a^1, a^{-1}, a^2, a^{-2}, \ldots\} \in G$.

$\Rightarrow \{a^i \mid i \in \mathbb{Z}\} \subseteq G$.

- $(S_3, \cdot)$ not cyclic.

as $O(S_3) = 6$ & $\exists$ no element in S_3 having order 6.

$O(G) = n$, G finite cyclic

$G = \langle a \rangle$

# of generator of $G = \phi(n)$.

of +ve integer $< n$ & coprime to n.

Example:- Let G be an abelian gr. of order 6 containing an element of order 3. Prove that G is a cyclic group.

if G is even order group no. of order 2 element is always odd

Sol^n:- $O(G) = 6$

let $a \in G$ s.t. $O(a) = 3$

As G is even order group, $\exists$ atleast one order 2 element in G.

let $b \in G$, s.t. $O(b) = 2$.

if $a, b \in G$ & $ab = ba$

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

then $O(ab) = O(a) \cdot O(b)$.

$\Rightarrow G = \langle ab \rangle$.

Example:- let G be an infinite cyclic gr. generated by a. Prove that a & a^{-1} are the only generators of the group.

Sol^n:- let $G = \langle b \rangle$, $b \neq a, a^{-1}$

Then $a = b^p$ for some integer p.

Also $G = \langle a \rangle$

$\Rightarrow b = a^m$ for some integer m. otherwise $O(b)$ will be finite.

So, $b = a^m = b^{pm} \Rightarrow b^{pm-1} = e \Rightarrow pm - 1 = 0$ as G is infinite cyclic group.

$\Rightarrow pm = 1$

$\Rightarrow p = 1, m = 1$.

Theorem Let $(G, \cdot)$ be a finite cyclic group generated by a. Then a^r, r some +ve integer, is a generator of a iff $r < n$ & $\gcd(r, n) = 1$.

Proof of the theorem:- $G = \langle a \rangle$, let $O(a) = n$

Then $O(a) = n$ & $G = \{a, a^2, a^3, \ldots a^n (= e)\}$

let a^r be a generator of G.

$\Rightarrow a^r \in G = \{a, a^2, \ldots a^n (= e)\} \Rightarrow r < n$.

Now, $G = \langle a^r \rangle$ & $a \in G$.

$\Rightarrow a = (a^r)^m$ for some integer m.

$\Rightarrow a^{mr-1} = e$.

As $O(a) = n$, we must have $n \mid (mr - 1)$.

i.e. $mr - 1 = nk$ for some integer k.

$\Rightarrow mr + nk = 1$. $\Rightarrow G = \langle a \cdot b \rangle$.

$\Rightarrow \gcd(r, n) = 1$

Converse

let $r < n$, coprime to n.

$$O(a^r) = \frac{O(a)}{\gcd(r, O(a))} = \frac{n}{\gcd(r, n)} = n = O(a)$$

$\Rightarrow a^r$ is also a generator of G.

Example: S = the set of n^{th} root of unity.

$= \{x \in \mathbb{C} \mid x^n = 1\}$.

Show that $(S, \cdot)$ is a cyclic group.

Sol^n:

- $(S, \cdot)$ is a group. Exercise.
- $(S, \cdot)$ is cyclic : $S = (1, x, x^2, x^3, \ldots, x^{n-1})$

$x^n = 1 = \cos 0 + i \sin 0$

$x = \cos\left(\frac{2k\pi + 0}{n}\right) + i \sin\left(\frac{2k\pi + 0}{n}\right) \Rightarrow O(S) = n$.

$k = 0, 1, 2, \ldots, n-1$

$\alpha = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$

Also, $O(\alpha) = n$!!

So, S is cyclic.

$Z_n^* = \{a \in Z_n \mid \gcd(a, n) = 1, a < n\}$; $|Z_n^*| = \phi(n)$.

(set of all units mod n)

($\exists x \in Z_n$ s.t. $ax \bmod n = 1$)

$(Z_n^*, \cdot)$ forms a group. $\quad a, a^2, a^3, \ldots, a^{\phi(n)} = 1$

$\alpha \to$ Primitive root mod n or primitive element of Z_n^* or generator of Z_n^*

$\alpha \in Z_n^*$ is a primitive root mod n if $O(\alpha) = \phi(n)$.

Euler's Theorem

$\gcd(a, n) = 1$

$a^{\phi(n)} = 1 \pmod n$.

Example: $Z_8^* = \{1, 3, 5, 7\}$.

$0, 1, \ldots, 7$.

$\phi(8) = \phi(2^3) = 2^3\left(1 - \frac{1}{2}\right) = 2^3 \times \frac{1}{2} = 4$

$\alpha = 1$
$\alpha = 3$
$\alpha = 5$
$\alpha = 7$

$a^k \bmod 8$

	$k=1$	$k=2$	$k=3$	$k=4$
$a=1$	[1]	1	1	1
$a=3$	3	[1]	3	1
$a=5$	5	[1]	5	1
$a=7$	7	[1]	7	1

Fact: (properties of generator of Z_n^*).

(i) Z_n^* has a generator iff $n = 2, 4, p^k$ or $2p^k$, p is odd integer, $k \geq 1$

not cyclic: Z_8^* $n = 8 = 2^3$; Z_{21}^* $n = 21 = 7 \times 3$

(ii) if α is a generator of Z_n^*, then $Z_n^* = \{\alpha^i \bmod n \mid 0 \leq i \leq \phi(n) - 1\}$ — Z_n^* is cyclic.

(iii) if α is a generator of Z_n^*, then $b = \alpha^i$ is also a generator iff $\gcd(i, \phi(n)) = 1$ → $\phi(Z_n^*) = \phi(n)$.

Z_n^* has $\phi(\phi(n))$ many generators.

(iv) $\alpha \in Z_n^*$ is a generator of Z_n^* iff $\alpha^{\frac{\phi(n)}{p}} \not\equiv 1 \pmod n$ for each prime divisor p of $\phi(n)$.

Theorem (Determining primitive roots when they exist).

a) If g is a primitive root mod an odd prime power p^k, then g or $g+p^k$ (which ever odd) will be a primitive root mod $2p^k$.

b) If g is a primitive root mod mod an odd prime p, Then g or $g+p$ (whichever odd) will be a primitive root mod p^2.

c) If g is a primitive root mod p^2 when p is an odd prime, the g is a prime root mod any higher power p^k of p.

Theorem (Determining primitive roots when they exist).

a) If g is a primitive root mod an odd prime power p^k, then g or $g+p^k$ (which ever odd) will be a primitive root mod $2p^k$.

b) If g is a primitive root mod mod an odd prime p, Then g or $g+p$ (whichever odd) will be a primitive root mod p^2.

c) If g is a primitive root mod p^2 when p is an odd prime, the g is a prime root mod any higher power p^k of p.

6/8/18

$\phi(p) = p-1$, if p prime

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

if $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$.

$\phi(mn) = \phi(m)\phi(n)$ when $\gcd(m,n) = 1$.

> if $a^k \equiv 1 \pmod n$
> then $o(a) \mid k$

Example: a) Verify that $g = 3$ is a primitive root of 223.

$Z^*_{223} = o(Z^*_{223}) = \phi(223) = 222$.

(1) Check $o(3) = \phi(223) = 2 \times 3 \times 37$.

i.e to check that

$3^2, 3^3, 3^{37}, 3^{2\times 3}, 3^{2\times 37}, 3^{3\times 37} \not\equiv 1 \pmod{223}$

$3^{222} = 1 \pmod{223}$

c) Euler's theorem

$a^{\phi(n)} = 1 \pmod{n}$ when $\gcd(a,n) = 1$

$O(a) \mid \phi(n)$.

$O(a) = 10$

$10 \mid \phi(223) = 222$

No. order 10 element mod 223.

d) $\phi(\phi(223)) = \phi(222) = \phi(2 \times 3 \times 37)$

$= \phi(2) \cdot \phi(3) \cdot \phi(37) = 1 \times 2 \times 36 = 72$.

b) algo order of power formula.

Example $\forall$ +ve integer n, $\exists$ a cyclic group.

S = the set of nth root of unity.

$= \{ x \in C \mid x^n = 1 \}$

is a cyclic group.

Elliptic Curve group

E/Z_p : $y^2 = x^3 + ax + b$ are Z_p, $p > 3$ be a prime.

Elliptic curve ① is the set of sol^{n}s $(x,y) \in Z_p \times Z_p$ to the congruence $y^2 = x^3 + ax + b \pmod{p}$.

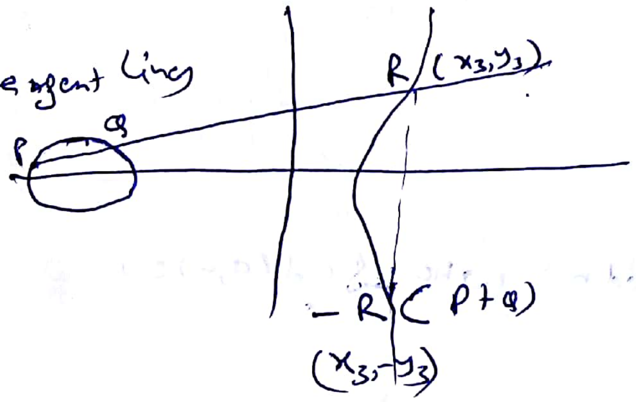
when $a, b \in Z_p$ are constants satisfying $4a^3 + 27b^2 \neq 0 \pmod{p}$.

together with a special pt. ⓗ, called point of infinity.

Point add^n :-

↓

Chord & tangent line



$PQ = y = mx + \lambda$

$E/Z_p = y^2 = x^3 + ax + b.$

$(mx + \lambda)^2 = x^3 + ax + b.$

$x^3 - m^2x^2 + (a - 2m\lambda)x + b - \lambda^2 = 0.$

$x_1 + x_2 + x_3 = m^2.$

$x_3 = m^2 - (x_1 + x_2)$; $y_3 = mx_3 + \lambda$

$P + Q = (x_3, -y_3)$

- $E/Z_p = y^2 = x^3 + ax + b,\ 4a^3 + 27b^2 \neq 0,\ a, b \in Z_p.$

- if $p = (x_1, y_1) \neq \Theta$ then $-p = (x_1, -y_1)$

if $p = (x_1, y_1) \neq \Theta$ then $Q = (x_2, y_2) \neq \Theta,\ p \neq -Q,$

then $p + Q = (x_3, y_3)$ with

$x_3 = m^2 - x_1 - x_2$

$y_3 = m(x_1 - x_3) - y_1$

when $m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } p \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & \text{if } p = Q. \end{cases}$

if $p = \Theta$ then

$p + \Theta = \Theta + p = p.$

Θ → additive identity

or

pt. at infinity

→ third pt. of intersection of any vertical line with the curve.

Scanned by CamScanner

Theorem:- $(E/Z_p, +)$ forms an abelian group.

Example :- $E/Z_{11} : y^2 = x^3 + 7x + 5$.

Determine all the points on E.

x	$x^3+7x+5 \bmod 11$	in QR(11)	y	$(11-4)=7$
0	5	Yes	4, -4	$1^2 \equiv 1 \bmod 11$
1	2	No		$2^2 = 4 \bmod 11$
2	5	Yes	4, -4	
3	9	Yes	3, -3	$3^2 = 9 \bmod 11$
4	9	Yes	3, -3	
5	0	—	0	$4^2 = 16 = 5 \bmod 11$
6	10	No		$5^2 = 25 = 3 \bmod 11$
7	1	Yes	1, -1	$6^3 = 36 = 3 \bmod 11$
8	1	Yes	1, -1	
9	5	Yes	4, -4	$QR(11) = \{1, 4, 9, 5, 3\}$.
10	8	No		

$\Rightarrow$ Square mod 11.

$(0,4)(0,7)$

$(2,4)(2,7)$

Add to ∞

$O(E) = 14 + 1 + 1 = 16$.

$(5,0)$

9/4/18

Elliptic Curve group:-

- Point Counting
- Doubling, Addtn
- finding Order of a point

$E/Z_p : y^2 = x^3 + ax + b$, $a, b \in Z_p$, $4a^3 + 27b^2 \neq 0 \bmod p$.

— (1)

all pts. $(x, y) \in Z_p \times Z_p$ satisfying (1), together with pt of infinity (∞) forms an abelian group under + defined as follows.

Given $P(x_1, y_1)$, $Q(x_2, y_2)$,

$P + Q (x_3, y_3)$ where

$$x_3 = m^2 - x_1 - x_2$$
$$+y_3 = m(x_1 - x_3) - y_1$$

$$m = \frac{y_2 - y_1}{x_2 - x_1} \text{ if } P \neq Q$$
$$\frac{3x_1^2 + 7}{2y_1}$$

Example:-

$E/Z_{11} : y^2 = x^3 + 7x + 5$

Find 10P when $P = (2, 4)$

$(10)_{10} = (1010)_2$

$10P = 8P + 2P$.

$2^0 P = (2, 4)$
$2^1 P = (8, 1)$
$2^2 P = 4P = (9, 9)$
$2^3 P = 8P = (5, 0)$
$2^4 P = 16P = 8P + 8P =$ (∞)

Calculate $2P (x_3, y_3)$

$$m = \frac{3 \cdot 2^2 + 7}{2 \cdot 4} = 19 \cdot 8^{-1} \bmod 11$$
$$= 8 \times 7 \bmod 11$$

$x_3 = 1^2 - 2 - 2 = 1 - 4 = -3 = 8 \bmod 11 = 1 \bmod 11$

$y_3 = 1(2 - 8) - 4 = -6 - 4$
$= -10 \bmod 11$
$= 1 \bmod 11$

$10P = 8P + 2P$.

$= (8, 1) + (8, 10) = (2, 7)$

$\# E/_{211} = 16$.

Ord. $E((2,4))/16$.

$\Rightarrow 2, 4, 8, 16$.

$P \in E$. Cyclic group → yes. generated by $(2,4)$

$Ord_E(P)$ = least $+ve$ int n.

s.t. $nP = \mathcal{O}$.

$G \rightarrow$ a grp of order $; a \in G$.

Then $O(a) \mid n$

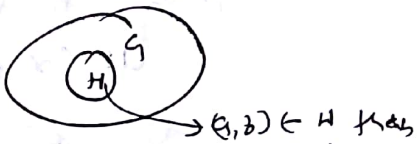
Abt today class ⇒

Exercise $Ord_E((0,y)) = ?$

Subgroup $(G, \circ)$ group

$H \subseteq G$, non empty subset of G

$(H, \circ)$ forms a group itself



then $(a \circ b) \in H$.

Fact : # Same identity e as in G $\in H$.

Same inverse a^{-1} as in G of $a \in H$.

Fact :- $(G, \circ)$ gr., $H \subseteq G$.

(i) $a, b \in H \Rightarrow a \circ b \in H$

(ii) $a \in H \Rightarrow a^{-1} \in H$.

↳ H is a subgroup of G.

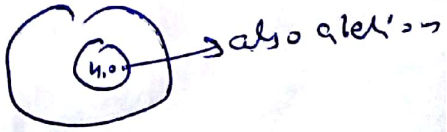
$a, b \in H \Rightarrow a \circ b^{-1} \in H$

Eg! $(G, \circ)$ finite gr $H \subseteq G$;

$a, b \in H \Rightarrow a \circ b \in H$ does not hold if G is infinite.

(i) H is a subgroup of G

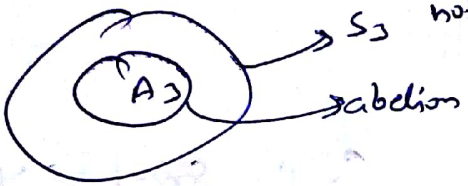
$(G, \circ)$ abelian



Eg. $G = (\mathbb{Z}, +)$ gr.

$\mathbb{N} \subseteq \mathbb{Z}$

$(\mathbb{N}, +)$ → not group.



Theorem:- Every subgroup of a cyclic gr. is cyclic.

proof:- Let $(G,\circ)$ be a cyclic gr. $G = \langle a \rangle$

Let $(H,\circ)$ be a subgroup of G.

Case 1 $H = G$ →

Case 2 $H = \{e\} = \{e^n : e \mid n \in \mathbb{Z}\}$. } trivial.

Case 3 H is a proper subgroup of G.

Then H must have an element in it other than e.

Let $(x \neq e) \in H$.

So, $x^{-1} \in H$ as H is itself a group.

As $x \in G$, we have $x = a^k \in H$ for some $k \in \mathbb{Z}$.

Also $x^{-1} \in G \Rightarrow x^{-1} = a^{-k} \in H$

So, $a^k, a^{-k} \in H$ for some $k \neq 0$.

So, there are some +ve integral power of a in H.

Let m = least such +ve integer s.t. $a^m \in H$.

(by well-ordering principle)

Claim, $H = \langle a^m \rangle$

Take $b \in H$

Then $b = a^b$ for some b as $b \in G$

$= \langle a \rangle, b \geq m$.

By division alg.

$b = mq + r$, $0 \leq r < m$.

$a^b \in H, a^{mq} \in H$

$\Rightarrow a^b \circ a^{-mq} \in H$

$\Rightarrow a^r \in H \Rightarrow r = 0$.

$h = (a^m)^q$

Note:- If a subgr. H of a finite gr. $G = \langle a \rangle$ of order n is generated by a^m, then $m \mid n$.

Theorem:- A cyclic gr. of prime order has non-trivial subgrps.

10/4/13

Fact H, K subgroup of G.

$H \cap K$ subgroup of G? Yes. $a, b \in H \cap K$

HUK? NO To prove that $a \cdot b^{-1} \in H \cap K$.

$G = (\mathbb{Z}, +)$, $H = (2\mathbb{Z}, +)$, $K = (3\mathbb{Z}, +)$

K → subgroup of G.

$2 \in HUK$, $3 \in HUK$, $2 + 3 = 5 \notin HUK$

Fact:- H, K subgroup of G

$\Rightarrow HUK$ subgroup of G, iff $H \subseteq K$ or $K \subseteq H$.

→ gr. of prime order → always cyclic, $\langle a \rangle$, $o(a) = |G|$

G, $o(G) = p$ = prime.

# of generators :- $\phi(p) = p - 1$.

G → cyclic group of order n

# of generator $= \phi(n)$.

Fact:- Every element (te) itself is a generator of a prime order gr.

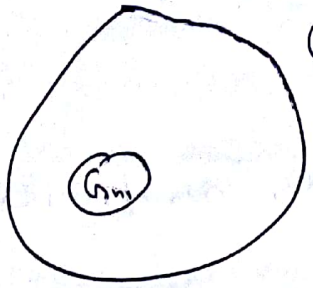
e.g. $Z_{11} = \{0, 1, 2, \ldots, 10\}$, $(Z_{11} - \{0\}, \cdot)$ cyclic grp. $= \{1, 3, 3, \ldots 10\}$.

with 'identity' 1.

# of generator $= \phi(10) = \phi(5 \times 2)$

$= \phi(5) \cdot \phi(2)$

$= 4 \times 1 = 4$.



$(G, \cdot)$ cyclic

$O(G) = n = n_1 n_2 \cdots n_k$.

Theorem: A cyclic group of order n has one & only one subgroup of order d for every +ve divisor d of n.

Proof: $G = \langle a \rangle$ cyclic, $O(G) = n : O(a)$

Then $G = \{a, a^2, \ldots a^n (= e)\}$.

Case 1: $d = 1$ → $\{e\}$ → only subgr. of order 1.

Case 2: $d = n$ → G → only subgr. of order n.

$Z_{13}^* = Z_{13} - \{0\}$, mult. cyclic gr.

$O(Z_{13}^*) = 12 = 2 \times 3 \times 2$

How many cyclic subgroups?

Order → 1, 2, 3, 4, 6, 12

Let $1 < d < n$ be a +ve divisor of n i.e. $n = md$ for some positive integer m.

Now, $a^m \in G$ & $O(a^m) = \dfrac{O(a)}{\gcd(m, O(a))} = \dfrac{n}{\gcd(m, n)}$

$= \dfrac{n}{m} = d$.

$H = \langle a^m \rangle$, $O(a^m) = d$.

Cyclic subgroup of G of order d.

Uniqueness

Let H' be another subgroup of G with $O(H') = d$

G cyclic $\Rightarrow H'$ cyclic

$\langle a \rangle$

Let b be the least positive integer s.t. $a^b \in H'$

Then $H' = \langle a^b \rangle$.

$\Rightarrow a^{bd} = e$

$G = \{a, a^2, \ldots a^n = e\}$, $\boxed{G = \langle a \rangle, \; O(G) = n}$

$\Downarrow$

$a^n = e$

By div. algo,

$b = mq + r, \; 0 \le r < m < b$, ($q, r$ unique)

b & m q d ord

$a^b = a^{mq} \cdot a^r \Rightarrow a^{rd} = e$

$\Rightarrow r = 0$

$b = mq$

$\langle a^b \rangle \subseteq \langle a^m \rangle$

$\downarrow H' \qquad \downarrow H$

Also,

$O(H') = d = O(H)$

$\Rightarrow H' = H$

$b = mq$

$\langle a^b \rangle \subseteq \langle a^m \rangle$

order $= d =$ order

Ring $(R, +, \cdot)$ → $(R, +)$ abelian gr.
→ $(R, \cdot)$ Semigroup
→ left & right distributive laws hold.

$\begin{cases} a.(b+c) = a.b + a.c \\ (a+b).c = ac + b.c \end{cases}$

Field :- $(F, +, \cdot)$ → $(F, +)$ abelian gr.
→ $(F - \{0\}, \cdot)$ abelian gr.
→ distributive laws hold.

e.g. $(\mathbb{Z}, +, \cdot) \rightarrow$ Ring

$(\mathbb{Z}_n, +, \cdot) \rightarrow$ Ring.

a^{-1} exists provided $\gcd(a, n) = 1$

$(\mathbb{Z}_p - \{0\}, +, \cdot)$, p is prime is a field.

- Polynomical ring
- Galois field Construction
- Finite field.

Theorem (Existence & Uniqueness)

(i) If F is a finite field, the F has p^m elements for some prime p & integer $m \geq 1$.

(ii) for every prime order p^m, there is a unique (upto isomorphism) finite field of order p^m. This field is denoted by F_p^m, or sometimes $GF(p^m)$.

$\phi : F \to F'$

$\phi(a \circ b) = \phi(a) * \phi(b)$

$F = \{a_1, a_2, \ldots a_n\}$ ϕ

$F' = \{b_1, b_2 \ldots b_n\}$

$R \to$ ring (commutative)

$R[x] \to$ also ring, called poly ring. $a_i \in \mathbb{Z}_p$; $a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$.

$GF(p) = \mathbb{Z}_p$

$\downarrow$

$GF(p^m)$.

Building finite field from $\mathbb{Z}_p(x)$

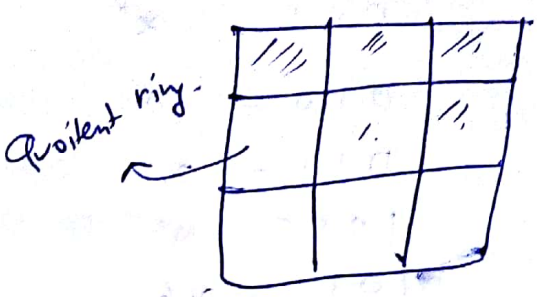
	Integer ($\mathbb{Z}$)	polynomial
→ infinite ring		$\mathbb{Z}_p(x)$
fixed ring element	m (int > 1) ←	m (poly of deg > 0)
finite module ring	$\mathbb{Z}_m$	$\mathbb{Z}_p(x) \pmod m$
When is finite module ring a field?	m = a prime	$\mathbb{Z}_p[x] \pmod m$ is field iff m is an irreducible poly

$g(x) \bmod f(x)$ → deg k.

deg < k.

$f(x) = h(x)q(x) + r(x)$

$0 \le \deg r(x) < \deg h(x)$



Example:- GF(2^2) Construction

$Z_2[x]/(m)$ → irreducible poly of deg 2.

GF(p^m)

x^2, x^2+1, x^2+x, x^2+x+1

$x^2+1 = (x+1)(x+1)$ — reducible

$= x^2+2x$

x^2+x+1 — irreducible

GF(p) = Z_p

$Z_p[x]/$(irreducible poly of degree m)

$Z_2[x]$ → all poly's with coeff. from $Z_2 = \{0,1\}$.

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

$= 1 \pmod x$

$f(x)g(x) = 1 \pmod{(x+1)}$

GF(2^2) = GF(4) = $Z_2[x]/x^2+x+1$

$= \{0, 1, x, x+1\}$

Power x^2.

poly	Binary	Power
0	00	
1	01	x^0
x	10	x
x+1	11	x^2
	x^1 x^0	

$x^2+x+1 = 0$

$x^2+1 = -x = x \bmod 2$.

GF(2^3) = GF(8)

$Z_2[x]/(m)$ → irreducible deg 3 poly

Example:- GF(8) = GF(2^3) Construction

$= Z_2[x]/(f(x))$ → irreducible of deg 3.

$= \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$

Check ⟹ $f(x) = x^3+x+1$ or x^3+x^2+1

Poly	x^2 x 1 Binary	power
0	0 0 0	—
1	0 0 1	x^0
x	0 1 0	x
$x+1$	0 1 1	x^3
x^2	1 0 0	x^2
x^2+1	1 0 1	x^6
x^2+x	1 1 0	x^4
x^2+x+1	1 1 1	x^5

$x^3 = x+1$ → $x^6 = (x+1)^2$
$= x^2+2x+1 = x^2+1$

$x^4 = x(x+1) = x^2+x$

$x^5 = x^3 + x^2$
$= x+1+x^2$.

$GF(p^m) = Z_p[x]/(f(x))$

order of this field.

$\deg f(x) = m$; irreducible.

$\{0, 1, 2, \ldots, p-1\}$; $a_0 + a_1 x + \ldots + a_r x^r$ $r < m$