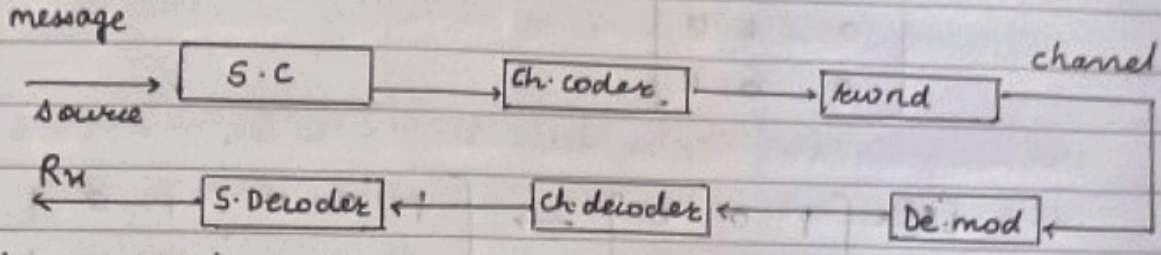
- Error Control coding :-



- Linear block code

Q. - $n = 6$, $k = 3$, for (6,3) linear block code

$k = 3$, Three message bits $d = \{d_1, d_2, d_3\}$

↳ Block of data

→ (message, k bits)(Parity bit, r bits) — codeword

→ Combinational ckt

→ No memory

- Convulated code

(n, k, m)

↑ memory elements

$[D]_{1 \times k}$ ..... row matrix i/p

$[C]_{1 \times n}$ code word o/p

$[G] = [I_k : P]$

$k \times k$ $k \times r$

Identity matrix — Parity Matrix

$$[G] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$[G] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \longrightarrow \left[\begin{array}{ccc:ccc} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right]$$

P

$$[G] = [\, I_{K\times K} \vdots P_{K\times n} \,]$$

$I_{K\times K}$ ↑ Identity matrix

$P_{K\times n}$ ↖ Parity matrix

- Encoding

$$[C] = [D][G]$$

$[D]_{1\times K}$ $[C]_{1\times n}$

d_1	d_2	d_3	d_1	d_2	d_3	$d_1 \oplus d_3$	$d_2 \oplus d_3$	$d_1 \oplus d_2$
0	0	0	0	0	0	0	0	0
0	0	1	0	0	1	1	1	0
0	1	0	0	1	0	0	1	1
1 ← 0	1	1	0	1	1	1	0	1
1 ← 0	0	0	1	0	0	1	0	1
1 ← 0	0	1	1	0	1	0	1	1
1 ← 0	1	0	1	1	0	1	1	0
1	1	1	1	1	1	0	0	0

Q. Determine the set of codewords for (7,4) block code with [G]

$$[G] = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$[C]_{1\times n} = [D]_{1\times k} \times [G]_{k\times n}$

$[d_0 \; d_1 \; d_2 \; d_3 \; d_0 \oplus d_2 \oplus d_3 \; d_0 \oplus d_1 \oplus d_2 \; d_1 \oplus d_2 \oplus d_3]$

d_0	d_1	d_2	d_3	c_0	c_1	c_2	c_3	c_4	c_5	c_6	hanning weight
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1	1	0	1	3
0	0	1	0	0	0	1	0	1	1	1	4
0	0	1	1	0	0	1	1	0	1	0	3
0	1	0	0	0	1	0	0	0	1	1	3
0	1	0	1	0	1	0	1	1	1	0	4
0	1	1	0	0	1	1	0	1	0	0	3
0	1	1	1	0	1	1	1	0	0	1	4
1	0	0	0	1	0	0	0	1	1	0	3
1	0	0	1	1	0	0	1	0	1	1	4
1	0	1	0	1	0	1	0	0	0	1	3
1	0	1	1	1	0	1	1	1	0	0	4
1	1	0	0	1	1	0	0	1	0	1	4
1	1	0	1	1	1	0	1	0	0	0	3
1	1	1	0	1	1	1	0	0	1	0	4
1	1	1	1	1	1	1	1	1	1	1	7

- Hamming Weight:- The total no of non-zero elements or no of 1's in code is defined as hamming weight of code

- Hamming distance: It is dist. betⁿ 2 codeword c_1 and c_2 and is defined as the no of places in which they differ and is denoted as:-

$$d(c_1, c_2)$$

Q. (6, 3) LCB

$$[G] = \left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right]$$

P I

a) Find parity hk matrix [H] systematic form
b) Encoding table for LBC
c) dmin
d) Errors detected
e) Errors can be corrected
f) Find syndrome decoding table

$k=3, n=6$ $[D]_{1\times k} = [d_1\ d_2\ d_3]$ data vector

$[C]_{1\times n} = [c_1\ c_2\ c_3\ c_4\ c_5\ c_6]$

$[d_1\ d_2\ d_3 - - -]$

$$[G]_{k\times n} = [P_{k\times(n-k)} : I_{k\times k}]$$

↑ parity bit

$$[H] = [P^T_{(n-k)\times k} : I_{(n-k)\times k}]$$

→a) $[H] = \left[\begin{array}{ccc|ccc} P^T & & & I & & \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$ or $\left[\begin{array}{ccc|ccc} I & & & P^T & & \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$

$[C] = [D][G]$

$$[d_1\ d_2\ d_3]\left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right]$$

$[d_1 \oplus d_3 \quad d_2 \oplus d_2 \quad d_2 \oplus d_3 \quad d_1 \quad d_2 \quad d_3]$

d_1	d_2	d_3	c_1	c_2	c_3	c_4	c_5	c_6	hanning weight
0	0	0	0	0	0	0	0	0	0
0	0	1	1	0	1	0	0	1	3
0	1	0	0	1	1	0	1	0	3
0	1	1	1	1	0	0	1	1	4
1	0	0	1	1	0	1	0	0	3
1	0	1	0	1	1	1	0	1	4
1	1	0	1	0	1	1	1	0	4
1	1	1	0	0	0	1	1	1	3

$d_{mm} = 3$ = Ans c)

Errors detected - $d_{mm} - 1$

$3 - 1 = 2 \Rightarrow$ d)

Error correction capability = $\frac{d_{mm}-1}{2}$

$\frac{3-1}{2} = 1 \Rightarrow$ e)

$$[H^T] = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$S = RH^T$

$$[0\ 0\ 0\ 1\ 0\ 1] \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$= [1\ 0\ 1]$

$E = 0\ 0\ 0\ 0\ 1\ 0$

$R = 0\ 0\ 0\ 1\ 0\ 1$

$C = R \oplus E$

$= 0\ 0\ 0\ 1\ 0\ 1 \oplus 0\ 0\ 0\ 0\ 1\ 0$

$= 0\ 0\ 0\ 1\ 1\ 1$

* Single error correcting

(n, k) Hanning Code $\rightarrow$ $(7,4)$ LBC

Code length $n \leq 2^{n-k} - 1$

$k \leq n - \log_2(n+1)$

No of parity bits $= (n-k)$

Error correcting capability. $t = \frac{d_{min}-1}{2}$

$n = 2^r - 1$

$k = 2^r - 1$

Q. Design a single error correcting code with a msg block of size 11 and show that by eg- it can correct single error

$k = 11$ $\quad\quad$ $(n, 11)$

$n \leq 2^{n-11} - 1$

$15 \leq 2^{15-11} - 1$

$15 \leq 2^4 - 1$

$15 \leq 16 - 1$

$15 = 15$

$(n, k) = (15, 11)$ - Hamming code

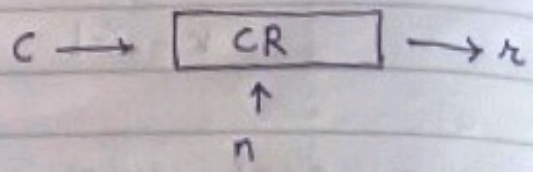
* Hamming bound

If an (n, k) linear block code is capable of correcting upto 't' errors, then total no of syndrome should not be less than the total no of all possible error pattern

Given - (n, k)

$s \Rightarrow 2^{n-k} \Rightarrow \sum_{i=0}^{t} {}^nC_i$

A binary code for which the hamming bound turns out to be an equality is called a perfect code



$$S = r \cdot H^T$$
$$= (C \oplus e) \cdot H^T$$
$$= CH^T \oplus C \cdot H^T$$
$$0 \oplus CH^T$$

Ex- Given (n, K) LBC (5, 2)

$$[G]_{(K,n)} = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{array}\right]$$

Find code vector

$$[C]_{1\times K} = [D]_{1\times K}\,[G]_{K\times n}$$

$$[d_1\ d_2] \left[\begin{array}{ccccc} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{array}\right]$$

$$[C] = [d_1\ d_2\ d_1 \oplus d_2\ d_2\ d_1]$$

Data Words		Code words					wt
d_1	d_2	c_1	c_2	c_3	c_4	c_5	
0	0	0	0	0	0	0	0
0	1	0	1	1	1	0	3
1	0	1	0	1	0	1	3
1	1	1	1	0	1	1	4

$[H] = [P^T : I_{(n-k)(n-k)}]$

$$\left[\begin{array}{cc:ccc} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

$$[H]^T = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$d_{min} = 3$

$t_{det} = d_{min} - \frac{1}{2}$

$= \frac{2}{2}$

$= 1$

- Std Array

coset leader ← Std Array →

Syndrome	c_0 00000	01110	10101	11011
S_1 101	e_1 10000	11110	00101	01011
S_2 110	e_2 01000	00110	11101	10011
S_3 100	e_3 00100	01010	10001	11111
S_4 010	e_4 00010	01100	10111	11001
S_5 001	e_5 00001	01111	10100	11010
		$(n,k) \rightarrow$	(5, 2)	

Systematic code where 1st 2 are msg bits and rest 3 are parity bits

00000, 01110, 10101, 11011

msg bits

011	00011	01101	10110	11000

⇓

Additional row where $S_4 \oplus S_5$ operation is taken combined

Coset leader ka addition taken in the same way as uppermost table

111	10010		

⇓

$S_1 \oplus S_2$, Combined addition

Coset addition remains same as the 1st table

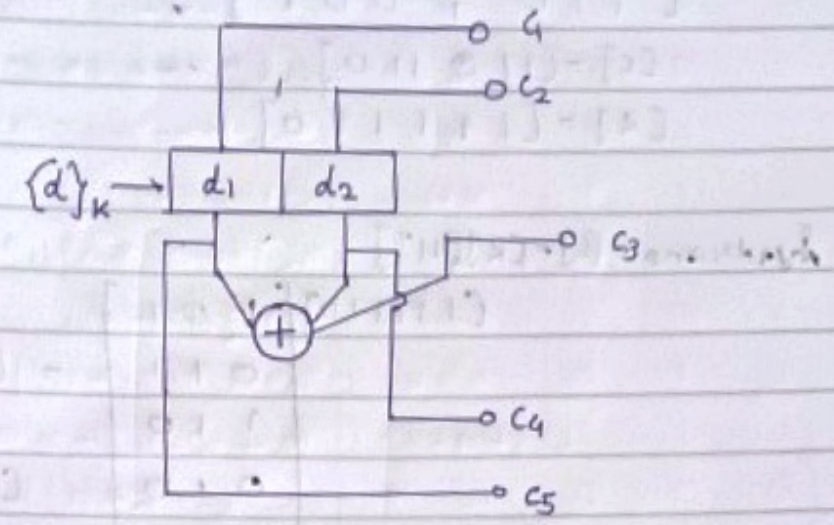
We did $S_4 \oplus S_5$ and $S_1 \oplus S_4$ bcoz we need 011 and 111 missing in the original std array table

$$C = D G$$

$$= [d_1 \; d_2] [G]$$

$$= [d_1 \; d_2, \; d_1 \oplus d_2, \; d_2, \; d_1]$$

Encoder diagram



$$S = r \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \rightarrow \text{available } s$$

$$[S_1 \; S_2 \; S_3] = [(r_1 r_2 r_3 \; r_4 \; r_5] \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$[S_1 \; S_2 \; S_3] = [(r_1 \oplus r_2 \oplus r_3), (r_2 \oplus r_4), (r_1 \oplus r_5)$$

continued after the following part

- Syndrome Decoding (remaining start part continued)

  If $C = C_1 \; C_2 \cdots C_n$ is a code vector (valid) transmitted over a noisy channel

  $R = r_1 r_2 \cdots r_n$ is the received code vector

Then error Pattern will be $E = R - C$ or $R = E + C$ (module 2)

$C = R + E$

$$[H] = \left[\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

$[C] = [1\ 1\ 0\ 1\ 1\ 0]$

$[R] = [1\ 1\ 1\ 1\ 1\ 0]$

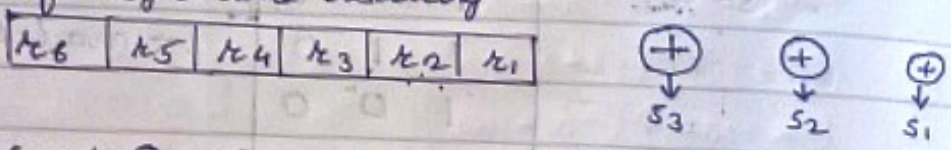
Syndrome $= [S] = [R][H^T]$

$$[1\ 1\ 1\ 1\ 1\ 0] \left[\begin{array}{ccc} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right] = [1\ 1\ 0]$$

$[100000]$

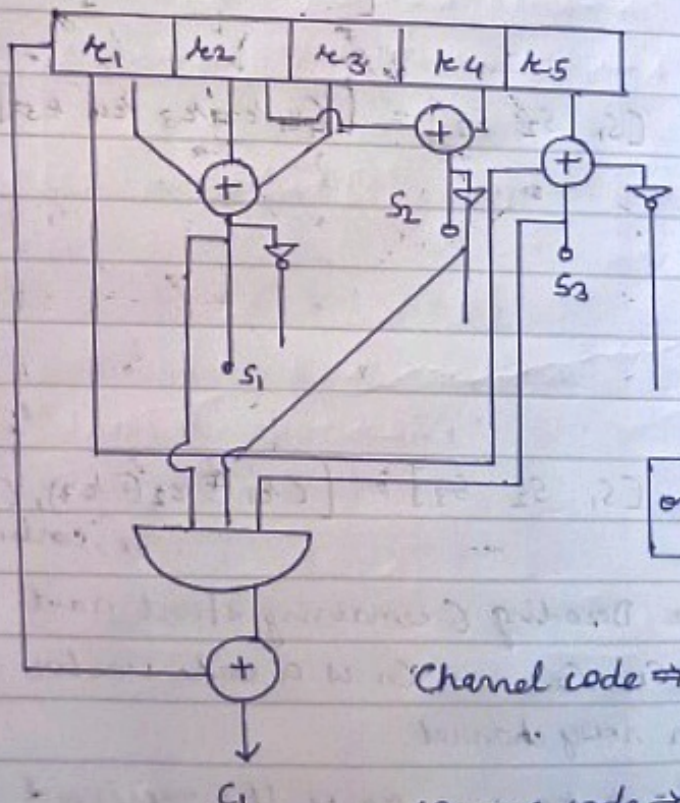
111110

- Diagram for syndrome decoding



$S_1 = r_1 \oplus r_3 \oplus r_4$, $S_2 = r_2 \oplus r_3 \oplus r_5$, $S_3 = Y_1 \oplus r_2$

- continued part



only for other code word

Channel code ⇒ Adds redundancy

source code ⇒ Removes Redundancy

- $(n, k) \rightarrow k$ message bits, $n \rightarrow$ coded bits, $(n-k) - r$ parity bits
  $(7,4)$ - Cyclic code

- $g(n)$ - generator Polynomial
  $h(n)$ - Parity

$(1+n^7)$

i.e $(1+n^7) \rightleftharpoons$

$\Downarrow$

$g(n) \cdot h(n)$

$(1+n^7) \rightleftharpoons (1+n+n^3) \rightarrow g(n)$.

$(n^{n+k} + \dots + 1)$

encoding $\rightarrow$ non-systematic

$C(n) = m(n) \cdot g(n)$

eg Consider Polynomial $(1+n^7)$ for $(7,4)$ cyclic code. It can be factorised as follows $(1+n^7) = (1+n)(1+n+n^3)(1+n^2+n^3)$
$\uparrow (g(n))$ polynomials
Find the coded word and coded in non-systematic format

$(7,4)$, $n = 7$, $k = 1$, $n-k = 3$

messages :-

message	m(x)	m(x) X g(x)	[c]
0 0 0 0	–	$0 \cdot (1+x+x^3) = 0$	0000000
0 0 0 1	1	$1 \cdot (1+x+x^3) = 1+x+x^3$	0001011
0 0 1 0	x	$x \cdot (1+x+x^3) = x+x^2+x^4$	0010110
0 0 1 1	$x+1$	$(x+1)(1+x+x^3) = 1+x+x^3+x^3+x^4$	0011101
0 1 0 0	x^2	$x^2(1+x+x^3) = x^2+x^3+x^5$	0101100
0 1 0 1	$1+x^2$	$1+x^2(1+x+x^3)$	0101100
0 1 1 0	x^2+x	$x^3+x(1+x+x^3)$	0111010
0 1 1 1	$1+x+x^2$	$(x+x^2+1)(1+x+x^3)$	0110001
1 0 0 0	x^3	$x^3(1+x+x^3)$	1011000
1 0 0 1	x^3+1	$x^3+1(1+x+x^3)$	1000011
1 0 1 0	x^3+x	$x^3+x(1+x+x^3)$	1001110
1 0 1 1	x^3+x+1	$(x^3+x+1)(1+x+x^3)$	1000101
1 1 0 0	x^3+x^2	$(x^3+x^2)(1+x+x^3)$	1011111
1 1 0 1	x^3+x^2+1	$(x^3+x^2+1)(1+x+x^3)$	1111111
1 1 1 0	x^3+x^2+x	$(x^3+x^2+x)(1+x+x^3)$	1100010
1 1 1 1	x^3+x^2+x+1	$(x^3+x^2+x+1)(1+x+x^3)$	1101001

systematic ctechique to find [c] – 1)

$$\frac{x^{n-k} \cdot m(x)}{g(x)}$$

$m(x) =$

$[m]_k = [0101] \Rightarrow m(x) = x^2+1$

$x^{n-k} = x^3$

$$\frac{x^3 \cdot (x^2+1)}{1+x+x^3} \rightarrow [0101] \qquad = \frac{x^5+x^3}{1+x+x^3}$$

x^5+x^3

$x^5+x^3+x^2$

$0+x^2 \leftarrow P(x)$ ∴ $[P]=100$

$[c]=[m][P]=[0101100]$

2) Obtain Generator matrix $[G]$ for the polynomial $1+x+x^3$

$[G]_{KXn}$

$$[G]_{kxn} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{matrix} x^3(g(x)) \\ x^2(g(x)) \\ x^1(g(x)) \\ x^0(g(x)) \end{matrix}$$

Write this in descending wise multiply karna i.e. $g(x)$

rotate x^0 wala row till x^3

$[0101]$ ↓ this is message

Is message ko $[G]$ se multiply karo column wise we will get $[c]$ for "non-systematic"

$$[G] = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

↓ I - we have to make this I using row and column transformation

$[G]_{KXn} = [I_{KXK} : P_{K(n-K)}]$

$$D(K) \quad \left[\underbrace{I_{4\times4}}_{D.\,4} : P_{4X}\right]$$

D(K) : We will get it as it as

$$[G]_{4\times 7} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$r_1 = r_1 \oplus r_3$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$\downarrow$

$$\left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right] \quad r_1 = r_1 \oplus r_4$$

$\downarrow$

$$\left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right] \quad r_2 = r_2 \oplus r_4$$

Q. Find generator and parity check matrices for (7,4) cyclic code for $g(x) = 1+x+x^3 = 1011$.

$x^3+x+1 = 1011$

→ $(7,4) = (n,k)$

$$[G]_{k\times n} = \begin{bmatrix} 1 & 0 & 1 & 1 & : & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & : & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & : & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & : & 0 & 1 & 1 \end{bmatrix}$$

$I_{k\times k}$

1st row = $x^{n-k}(g(x))$

2nd row = $x^{(n-k)-1}\, g(x)$

3rd row = $x^{(n-k)-2}\, g(x)$

4th row = $x^{(n-k)-3}\, g(x)$

$x^3(g(x)) = x^3(1+x+x^3) = x^6+x^4+x^3$

$x^2(g(x)) = x^2(1+x+x^3) = x^2+x^3+x^5 \longrightarrow$ @

$x\,g(x) = x(1+x+x^3) = x+x^2+x^4$

$1\cdot g(x) \quad 1\cdot(1+x+x^3) = 1+x+x^3$

Comparing @ with $G = \left[\begin{array}{cccc:ccc} 1 & 0 & 0 & 0 & - & - & - \\ 0 & 1 & 0 & 0 & - & - & - \\ 0 & 0 & 1 & 0 & - & - & - \\ 0 & 0 & 0 & 1 & - & - & - \end{array}\right]$

$\therefore G = [I \mid P]$

$c_1 = c_1 \oplus c_3$

$$\left[\begin{array}{cccc:ccc} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

$\downarrow$

$c_2 \rightarrow c_2 \oplus c_4$

$$\left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

$$r_1 \longrightarrow r_1 \oplus r_4$$

$$[G] = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

$\rightarrow$ $(x^7+1) = g(x) \cdot h(x)$

$(1+x+x^3)(h(x))$

$$h(x) = \frac{x^7+1}{x^3+x+1}$$

$$\begin{array}{r} x^4+x^2+x+1 \\ x^3+x+1 \overline{)\ x^7+1} \\ x^7+x^5+x^4 \\ \hline x^5+x^4+1 \\ x^5+x^3+x^2 \\ \hline x^4+x^3+x^2+1 \\ x^4+x^2+x \\ \hline x^3+x+1 \\ x^3+x+1 \\ \hline 0 \end{array}$$

$[H] = 10111$

$[H] = [P_{(n-k)\times k} : I_{(n-k)(n-k)}]$

$$H = \left[\begin{array}{cccc:ccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right] \begin{array}{l} 1 \\ 2 \\ (n-k)^{th} \text{ row} \end{array}$$

$I_{3\times3}$ ← $= n(n-k) = 3$

$[H] = [P^T \mid I_{k\times k}]$

① $R_2 \rightarrow R_2 \oplus R_3$

② $R_1 \rightarrow R_1 \oplus R_2$

↓

$$\left[\begin{array}{cccc:ccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right]$$

→ do the ① and ② operation we will get

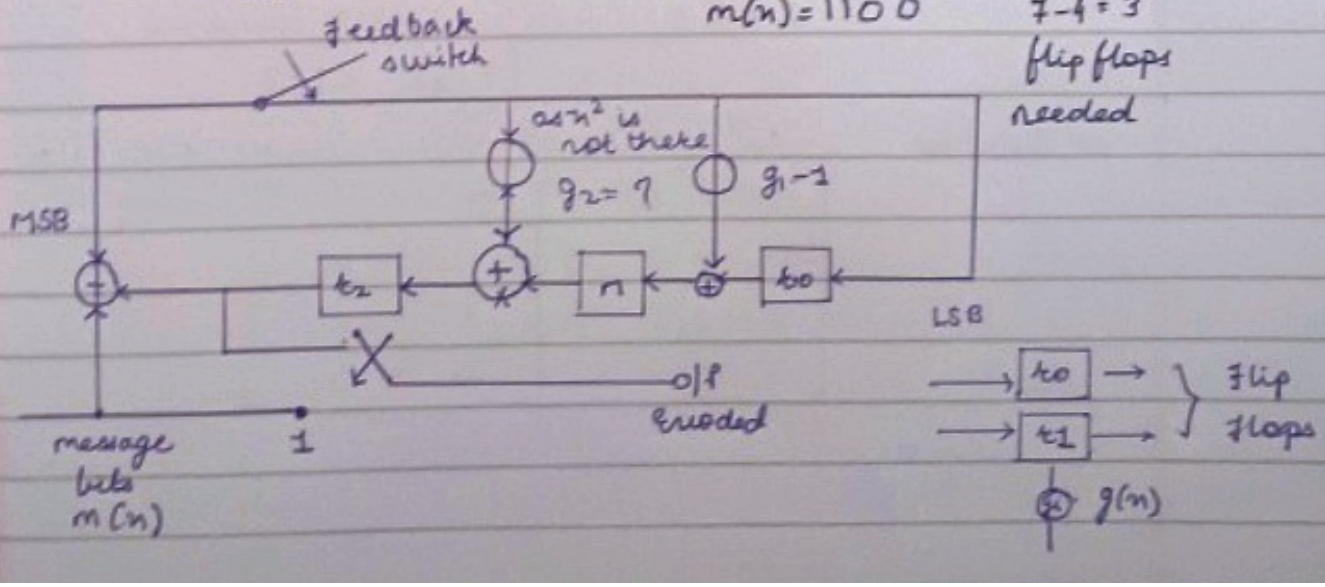
$$= \left[\begin{array}{cccc:ccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

3×3 I

- Design the encoder for $(n, k = 7, 4)$ cyclic code $g(n) = n^3 + n + 1$ and verify its operations for any msg vector

$m(n) = 1100$

$7 - 4 = 3$ flip flops needed



The contents of shift registers are shifted from i/p to o/p where clock pulse is applied

g_1, g_2 → represent closed path, if $g=1$ and open path if $g=0$ (no connection)

i/p	$t_2 = t_2'$	$t_1 = t_1'$	$t_0 = t_0'$	$t_2' = t_1$	$t_1' = t_0 \oplus t_2 \oplus m$	$t_2' =$
	0	0	0	0	0	0
1	0	0	0	0	$0 \oplus 0 \oplus 1 = 1$	1
1	0	1	1	1	0	1
0	1	0	1	0	0	1
0	0	0	1	0	1	0

$$\frac{x^{n-k} m(x)}{g(x)} = \frac{x^3(x^3+x^2)}{x^2+x+1}$$

$$= \frac{x^6+x^5}{x^3+x+1} = x$$

$$= 010$$

Q. Generator and parity check matrices of (7,4) cyclic codes for $g(x) = 1 + x + x^3$

$(n,k) = (7,4)$

$[G]_{k \times n} = [G]_{4 \times 7}$

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

$g(x) = (1) + 1(x) + 0(x^2) + 1(x^3) + 0(x^4) + 0x^5 + 0x^6$

$g(x) = 1101000$

$x(g(x)) = x(1 + x + x^3)$

$x + x^2 + x^4 = 0110100$

$x^2(g(x)) = x^2(1 + x + x^3)$

$= x^3 + x^2 + x^5 = 0011010$

$x^3 g(x) = x^3(1 + x + x^3) = x^3 + x^4 + x^6 = 0001101$

Now $[G] = \begin{matrix} g(x) \\ xg(x) \\ x^2(g(x)) \\ x^3 g(x) \end{matrix} \left[\begin{array}{cccc:ccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right] \begin{matrix} R_1 \\ R_2 \\ R_3 \\ R_4 \end{matrix}$ ... (1)

we know that

$[G] = [I_k : P]$

$t_2 = t_1 \oplus t_3$

$[G] = \left[\begin{array}{ccc:cccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right]$

$$[G] = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The systematic cyclic code-vectors can be formed by using

$$[V] = [D][G]$$

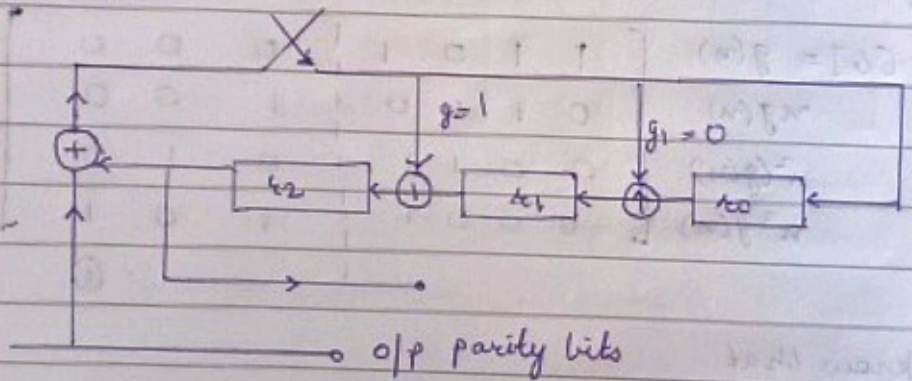
$$[d_0\ d_1\ d_2\ d_3] \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Q. Draw the encoder for generator polynomial for $1 + n^2 + n^3$

$n = 1001$

P → codeword

Encoder



i/p	r_2	r_1	r_0	$r_2' = m \oplus r_0 \oplus r_1$	$r_1' = r_0$	$r_0' = m \oplus r_2$
+	0	0	0			
0	1					
0	0					
+	0					
	1					

- $C(n) = d(n) \cdot g(n)$ — cyclic code
- $C = E \oplus R$ — corrected code word (LBC)
- $S = R \cdot H^T$
  ↓
  syndrome bits in LBC

$S(n)$ = Remainder of $\left[\frac{R(n)}{g(n)}\right]$
↓ generator polynomial

↑ data transmitted
$C = r \oplus E$
or
$\text{received}(n) = \text{transmitted}(n) + E(n)$ ①

$r = r \oplus E$
$r \rightarrow$ transmitted
or $r = r \oplus E$
$r(P) = r(P) \oplus E(P)$

$r(P) = m(P) g(P) \rightarrow$ non-systematic

$\frac{r(P)}{g(P)} = Q(P) + \frac{\text{remainder}(P)}{g(P)}$
quotient

$r(P) = m(P) g(P) + R(P)$
↓ remainder

$\frac{r(P)}{g(P)} = Q(P) + \frac{R(P)}{g(P)} \rightarrow S(P)$

$g(x) = 1+x^3+x^2$

Find the syndrome encoder / decoder ckt

Method 1 : To find syndrome

$$\text{remainder}\left[\frac{x(x)}{g(x)}\right] \quad \text{received code vector} = 1100110$$

$$\frac{x^{n-k}m(x)}{g(x)} - \frac{x^3 \cdot x^3}{1+x^2+x^3} = \frac{x^6}{1+x^2+x^3}$$

$$\begin{array}{r} x^3+x^2+x \\ x^3+x^2+1 \;\big)\; x^6 \\ \oplus\; x^6+x^5+x^3 \\ \hline x^5+x^3 \\ \oplus\; x^5+x^4+x^2 \\ \hline x^4+x^3+x^2 \\ \oplus\; x^4+x^3+x \\ \hline x^2+x = 110 \end{array}$$

$$\begin{array}{r} x^3+1 \\ x^3+x^2+1 \;\big)\; x^6+x^3+x^2+x \\ x^6+x^5+x^3 \\ \hline x^3+x^2+x \\ x^3+x^2+1 \\ \hline x+1 \;\rightarrow\; 011 \end{array}$$

	error pattern	Syndrome	$\frac{e(x)}{g(x)} = \frac{x^n}{x^3+x^2+1}$
MSB	x^6 1 0 0 0 0 0 0	1 1 0	x^6 / x^3+x^2+1
shift karo	x^5 0 1 0 0 0 0 0	0 1 1	x^5 / x^3+x^2+1
	x^4 0 0 1 0 0 0 0	1 1 1	x^4 / x^3+x^2+1
	x^3 0 0 0 1 0 0 0	1 0 1	x^3 / x^3+x^2+1
	x^2 0 0 0 0 1 0 0	1 0 0	x^2 / x^3+x^2+1
	x 0 0 0 0 0 1 0	0 1 0	x / x^3+x^2+1
	1 0 0 0 0 0 0 1	0 0 1	$1 / x^3+x^2+1$

S = (011) [binary approach] [Polynomial Approach]

error = 0100000

$e(x) = x^5$

r = 1100110

e = 0100000

c = r ⊕ e

= 1000110

$g(x) = x^3+x^2+1$

$x^3 + g_2x^2 + g_1x + 1$

received code (bits)	before shift S_0	S_1	S_2	after shift $S_0' = R \oplus S_1$	$S_1' = S_0$	$S_2' = S_1 \oplus S_2$
R	0	0	0	0	0	0
1	0	0	0	1	0	0
1	1	0	0	1	1	0
0	1	1	0	0	1	1

0	0	1	1	1	0	0
1	1	0	0	1	1	0
1	1	1	0	1	1	1
1	1	1	1	1	0	1

$S = 011$

as it is S_2' S_1' S_0'

- Cyclic Redundancy Code (CRC):

For the message sequence 1101001110,00 (14 bit)

parity polynomial $= 1 + x + x^3$

(1011) → (4 bits)

parity bits = 3 (n-k)

(7-4=3)

$$1011 \overline{)\ 11010011101100} \quad \leftarrow \text{in binary}$$

$$\frac{(x^{13} + x^{12} + x^{10} + x^7 + x^6 + x^5 + x^3 + x^2)(x^3)}{x^3 + x + 1} \rightarrow \text{in polynomial}$$

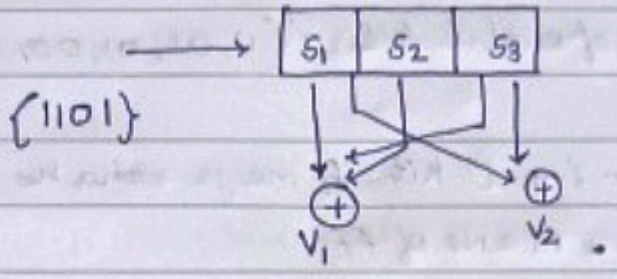
$= 100$

m | 100

14 bits

Convolution Code

Convolution Code is also called running code. It is also feed forward configuration



$g_1 = (1\,1\,1)$

$V_1 = S_1 \oplus S_2 \oplus S_3$

(M-1) no of zeroes to be appended to i/p seq so as to clear the ff's

$M = 3$

$\therefore M-1 = 2$

$\therefore 110100$

				$(S_1 \oplus S_2 \oplus S_3)$ = V_1	$(S_1 \oplus S_3)$ = V_2
i/p	S_1	S_2	S_3		
	0	0	0	0	0
1	1	0	0	1	1
1	1	1	0	0	1
0	0	1	1	0	1
1	1	0	1	0	0
0 →	0	1	0	1	0
0 →	0	0	1	1	1

{11, 01, 01, 00, 10, 11} → write in pair of 2-2 $(V_1 - V_2)$

Code Rate - $\frac{\text{input (no)}}{\text{no of output}}$

code rate $= \frac{1}{2}$

a) $(K+(M-1)).V$

$(4+2)\ 2 = 12$ - No of outbit bits - {11, 01, 01, 00, 10, 11}

3) Constrained length - Input kitne ff me ja raha he

= M = No of ff

Module Arithmetic

☐ mod m

ranges from 0 to m-1

The answer to this calculation is in always 0 to m-1 where m is called modulus

7 mod 11 - quotient 0
remainder = 7

20 mod 3 - Quotient = 6
remainder = 2

If a is negative then add as many multiples of n to get an answer range from 0 to m-1

$(a + (-a)) \bmod 10 = 0$
$(a \times a^{-1}) \bmod 10 = 1$

- $-3 \bmod 11 \rightarrow$ add 11 to -3
  $= 8$

- $-1 \bmod 11 = 10$

- Two numbers a and b are said to be congruent module n if $a \bmod n = b \bmod n$

$a \equiv b \bmod n$
↓
congruent

The difference between a and b will be multiple of n. So $a - b = kn$ for some values of k

$73 = 4 \bmod 23$

↓

$73 \bmod 23 = 4 \bmod 23$

↓

4

$4 \bmod 23 = 4$

$73 \bmod 23 = 4$

$a = 73$ $\quad \therefore (73-4) = 3 \times 23$

$b = 4$ $\quad k = 3$

$n = 23$

Q. $-1 = -6 \bmod 5$

In RHS multiple of 5 se multiply karo till lowest positive integer nai mila

$\therefore -6 + (5 \times 2) = 4$

$\therefore -6 \bmod 5 = 4$

$-1 \bmod 5 = 4$

$a = -1$ $\quad \therefore (a-b) = kn$

$b = -6$ $\quad \therefore 5 = k \times 5$

$k = 1$

. Properties of Congruencies

1) $a = b \bmod n$, $\quad n \mid a-b$

2) $a = b \pmod{} \Rightarrow b \equiv a \bmod (n)$

3) $a = b \pmod{n}$ and $b = c \pmod{n}$

4) $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$

5) $[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$

6) $(a \bmod n) \times b$ mo

. Properties based question

Q. $11 \bmod 8 = 3$

$15 \bmod 8 = 7$

Now apply ④ $10 \bmod 8 = 2$ = LHS

RHS - $26 \bmod 8 = 2$

. Modular division

. $5 \div 3 \bmod 11$

↓

We need to multiply 5 with inverse of 3 mod 11

$\frac{a}{b} = a \times \frac{1}{b}$

. $3 \times \square = 1 \bmod 11$ ∴ $3 \times n = 1 \bmod 11$ ∵ $(n = 11)$

3 × by aisa number jiska mod 11 lene pe 1 aye

- Euclid's Algorithm
- GCD(27,45)
- replace difference inplace of larger number

(27, 18) - difference inplace of larger no
(9, 18) - same
(9, 9)
↓
(9,0) → GCD is 9

Q. (17,41)
↓
(17,24)
(17,7)
(10,7)
(3,7)
(4,3)

When we will take difference of the two number (1,1)
↓
last pair

difference = 0
∴ HCF is 1

- Chinese Remainder theorem

If I have N chocolates

5 ÷ N → 1 chocolate left with me

$N \equiv 1 \mod 5$
$N \equiv 1 \mod 7$
$N \equiv 3 \mod 11$

To find common solution for all 3 we use chinese remainder

$X \equiv a_1 \bmod m_1$

$X \equiv a_2 \bmod m_2$

$X \equiv a_3 \bmod m_3$

$\vdots$

$M = m_1 \cdot m_2 \cdot m_3 \cdots m_n$

$M_1 = M / m_1$

$M_2 = M / m_2$

$M_3 = M / m_3$

$M = m_1 \cdot m_2 \cdot m_3$

$= 11 \times 5 \times 7$

$= 385$

$M_1 = 385 / 5 = 77$

$M_2 = 385 / 7 = 55$

$M_3 = 385 / 11 = 35$

$M = M_1 \cdot x_1 \cdot a_1 + M_2 \cdot x_2 \cdot a_2 + M_3 \cdot x_3 \cdot a_3$

x_1 - inverse of M_1

$M_1 \cdot x_1 \equiv 1 \bmod m_1$

we will write it as

$(x_1)\ (77 \bmod 5) = 1 \bmod 5$

$2 x_1 = 1 \bmod 5$

lowest value which satisfies

$\therefore x_1 = 3$

$M_2 \cdot x_2 = 1 \bmod m_2$

$(55 \bmod 7)\, x_2 = 1 \bmod 7$

$6 x_2 = 1 \bmod 7$

$x_2 = 6$

$M_3 \cdot x_3 = 1 \bmod 11$

$(35 \bmod 11) = 1 \bmod 11$

$2x_3 = 1 \bmod 11$

$x_3 = 6$

[$\because a \times a^{-1} = 1 \bmod c$]

$\therefore M = 77 \cdot 3 \cdot 1 + 55 \cdot 6 \cdot 1 + 35 \cdot 6 \cdot 3$

$= 1191$

$\therefore$ Final Answer $= M \mid m_1 m_2 m_3$

$= 1191 \mid 385$

↓

find by modulo division or difference method

(1191, 385)

(806, 385)

(421, 385)

(36, 385) → ab difference negative araha to next step nai karenge

$\therefore$ HCF = 36

Q. $x \equiv 1 \bmod 5$

$x \equiv 2 \bmod$

Q. $x \equiv 3 \bmod 5$

$x \equiv 6 \bmod 7$

$x \equiv 4 \bmod 11$

$M = 385$

$M_1 \cdot x_1 = 1 \bmod 5$

$(77 \bmod 5) x_1 = 1 \bmod 5$

$x_1 = 3$

$(55 \bmod 7) x_2 = 1 \bmod 7$

$x_2 = 6$

$(35 \bmod 11) x_3 = 1 \bmod 11$

$x_3 = 6$

$M = 77 \times 3 \times 3 + 55 \times 6 \times 6 + 35 \times 6 \times 4$

$693 + 1980 + 840$

$M = 3513$

$(m_1 m_2 m_3) = 385$

continue the process

(3513, 385)

(3128, 385)

(433, 385)

(48, 385)

↓ This is the answer

∴ 48 is the HCF

- Z_n → set of inv of additive
  Z_n^* → ... Multiplicative

$Z_n = Z_6$

$Z_6 \rightarrow 0$ to 5

$(a+b) \bmod z = 0$

$(a+a^{-1}) \bmod z = 1$

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

$Z_6^* = \{$

- Solve $(3x+4) \equiv 6 \bmod 13 - 4 \bmod 13$ $\quad a = kn$

$3x \equiv (6-4) \bmod 13$

GCD of 3 and 13 = 1

$GCD(3, 13) = 1$

$(3 \times \square) \bmod 13 \equiv 2$

$x = 5$

- Solve $14x \equiv 12 \bmod 18$

$a \equiv b \bmod c$; $a - b \equiv \bmod c$

$a = nc$

$(14x - 12) = 18c$

- Primeness :-

- Given number :-

Steps

1) Root find karo
2) find primes less than that
3) If the primes divide original no the number is not prime

- Euler's phi function

$\phi(n)$

↳ no of integer that are smaller than n and relatively prime to n

- When n is prime $Zn^* = \{0, \cdots n-1\}$

Properties

1) $\phi(1) = 0$
2) $\phi(p) = p-1$
3) $\phi(m \times n) = \phi(m) \times \phi(n)$

↳ m, n – relatively prime

4) $\phi(p^e) = p^e - p^{e-1}$

Q. What is value of $\phi(13)$

$\phi P=(P-1) = 13-1$

$= 12$

Q. $\phi(10) = \phi(2^1 \times 5^1)$

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

$(2-1) \times 5-1) = 4$

Q. $\phi(240) = 2^4 \times 3^1 \times 5^1$

$(2^4 - 2^3) \times (3^1 - 3^0) \times 5^1 - 5^0)$

$= 8 \times 2 \times 4$

$= 64$

Q. $\phi(49) = \phi(7) \times \phi(7)$

$= 6 \times 6$

$= 36$ ✗ wrong

$= 7^2 = p^e - p^{e-1}$

$7^2 - 7^1$

$= 42$

Q. What are the no of elements in Z_{14}^*

$\phi(14) = 7 \times 2$

$= (7-1) \times (2-1)$

$= 6$

. Fermat's little theorem

1st version

If 'p' → prime

and 'a' → integer

such that p does not divide a

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

$a^p \equiv a \bmod p$

Q. $6^{12} \bmod 11$

Write $6^{11-1} \equiv 1 \bmod 11 = 1$

$\therefore (6^{11-1} \bmod 11)(6^2 \bmod 11) \Rightarrow (1 \cdot 36) \bmod 11 = 3$

. Euler's theoram generalisation

1) Mod of Fermat's thm is prime
2) Euler's theoram has modulus as integer
3) $a^{\phi(n)} \equiv 1 \bmod n$

$a, n \rightarrow$ co-prime

4) $a^{(k \times \phi(n)+1)} = a \bmod n, \quad n = p \times q$

$a < n, k \rightarrow$ integer