DISCRETE STRUCTURES __/__/____

✱ NUMBER THEORY (Divisibility and Modular Arithmetic)

→ $a \equiv b \bmod m$; iff (i) $m \mid (a-b) = k$

(ii) $(a \bmod m) = (b \bmod m)$

→ $(a \overset{+}{\times} b) \bmod n = [(a \bmod n) \overset{+}{\times} (b \bmod n)] \bmod n$

• Modular Exponential.

E.g.: $23^{35} \bmod 19 = ?$

Soln:- power = $23 \bmod 19 = 4$

$x = 1$; $n = 19$ (always $x = 1$)

$(35)_{10} = (100011)_2$ (5 4 3 2 1 0)

binary place from r → l	x = 1	pow = 4	bin. number
i = 0	x = 4	pow = 16	1
i = 1	x = 7	pow = 9	1
i = 2	x = 7	pow = 5	0
i = 3	x = 7	pow = 6	0
i = 4	x = 7	pow = 17	0
i = 5	∴ x = 5		1

If bin. no. = 1 then $x = (x * pow) \bmod n$

$pow = (pow)^2 \bmod n$

∴ $23^{35} \bmod 19 = 5$

__/__/____

* EULER'S PHI FUNCTION:

Q.1. $\phi(13) = ?$

Soln:- 13 is a prime number

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

$\therefore \phi(13) = 13-1 = 12.$

Q.2. $\phi(10) = ?$

Soln:- 10 is a composite number.

Breaking 10 into multiples of prime numbers, $10 = 5 \times 2$

So, $\phi(10) = \phi(5 \times 2) = \phi(5) \times \phi(2) = 4 \times 1 = 4$

Q.3. $\phi(49) = ?$

Soln:- $\phi(49) = \phi(7 \times 7) = \phi(7^2)$

for prime p of power e, $\phi(p^e) = p^e - p^{e-1}$

So, $\phi(49) = \phi(7^2) = 7^2 - 7^1 = 42.$

Q.4. $\phi(240) = ?$

Soln:- $\phi(240) = \phi(2^4 \times 3 \times 5) = \phi(2^4) \times \phi(3) \times \phi(5)$

$= (2^4 - 2^3) \times 2 \times 4$

$= 64$

Q.5. $\phi(1^{10}) = ?$

Soln:- $\phi(1) = 0$ (Rule) Also, $\phi(1^{10}) = (1^{10} - 1^9) = 1 - 1 = 0$

$\therefore \phi(1^{10}) = 0.$

Theorems

1. $\phi(m \times n) = \phi(m) \times \phi(n) = (m-1)(n-1)$ $\quad m \neq n$, $m, n \to p$
2. $\phi(p^e) = p^e - p^{e-1}$
3. $\phi(1) = 0$

__/__/____

* FERMAT'S LITTLE THEOREM:

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

Q.1. $4^{532} \bmod 11 = ?$

Soln:- here, (mod 11) so, $n = 11$

So, $4^{n-1} = 4^{11-1} = 4^{10} \equiv 1 \pmod{11}$

i.e., $4^{10} \bmod 11 = 1$

Now,

$$4^{532} = 4^{(10 \times 53 + 2)} = (4^{10})^{53} \times 4^2$$

$$4^{532} \bmod 11 = (4^{10})^{53} \bmod 11 \times 4^2 \bmod 11$$

$$= (4^{10} \bmod 11)^{53} \times 4^2 \bmod 11$$

$$= (1)^{53} \times 16 \bmod 11$$

$$= 1 \times 5$$

$$\therefore 4^{532} \bmod 11 = 5$$

Q.2. $2^{50} \bmod 17$

Soln:- Here, $2^{16} \equiv 1 \bmod 17$

So, $2^{50} = 2^{16 \times 3 + 2}$

$$= (2^{16})^3 * (2)^2$$

$$= 1 * 2 \bmod 17$$

$$= 1 \times 2$$

$$= 2.$$

Q.3. $5^{18} \bmod 19$

Soln:- Satisfies theorem directly,

i.e., $5^{19-1} \equiv 1 \bmod 19$

$\Rightarrow 5^{18} \equiv 1 \bmod 19$

$\therefore 5^{18} \bmod 19 = 1$

Q.4. $5^{19} \bmod 19$

Soln:- $5^{19} \bmod 19$

$= (5^{18} \bmod 19) \times 5 \bmod 19$

$= 1 \times 5$

$= 5$

Q.5. If 3^{1000} is divided by 23, find its remainder.

Soln:- $\rightarrow (3^{1000} \bmod 23 = ?) \Rightarrow (3^{22} \bmod 23 = 1) \Rightarrow (3^{22})^{45} \times (3^{10}) \bmod 23 = 1 \times (59049 \bmod 23) = 8$

__/__/____

* Find the missing Check Digit for ISBN 10.

1. 0 6 1 8 2 6 9 4 1 $\boxed{x}$

Soln:-

0	6	1	8	2	6	9	4	1	x
×	×	×	×	×	×	×	×	×	×
10	9	8	7	6	5	4	3	2	1
"	"	"	"	"	"	"	"	"	"

$0 + 54 + 8 + 56 + 12 + 30 + 36 + 12 + 2 + x$

$= 210 + x$

ISBN10 is a mod 11 system. So, ~~dividing by 11~~

So, $210 + x$ = multiple of 11

getting as close to 210 with multiple of 11,

$11 \times 19 = 209$

$210 + 10 = 220 \longrightarrow 11 \times 20 = 220$

$11 \times 21 = 231$

$11 \times 22 = 242$

$11 \times 23 = 253$

$\therefore x = 10$ is check digit as well as missing digit.

2. 0 1 9 8 5 $\boxed{x}$ 8 0 3 0

Soln:-

0	1	9	8	5	x	8	0	3	0
×	×	×	×	×	×	×	×	×	×
10	9	8	7	6	5	4	3	2	1
"	"	"	"	"	"	"	"	"	"

$0 + 9 + 72 + 56 + 30 + 5x + 32 + 0 + 6 + 0$

$= 205 + 5x$

So, $205 + 5x$ = multiple of 11.

$205 + 5 \times 1 = 210$ ✗

$205 + 5 \times 2 = 215$ ✗

$205 + 5 \times 3 = 220$ ✓

$11 \times 19 = 209$

$11 \times 20 = 220$

$11 \times 21 = 231$

$11 \times 22 = 242$

$11 \times 23 = 253$

$x = (\text{multiple of } 11 - 205) \div 5$

$\therefore x = 3$ is not check digit. but missing digit

NOTE: CHECK DIGIT IS THE LAST DIGIT.

__/__/____

* Check digit for ISBN-13

Q. 9 7 8 0 5 4 5 5 6 7 4 7 [x]

Sol^{n}:- x x x x x x x x x x x x

1 3 1 3 1 3 1 3 1 3 1 3 1

$= 9+21+8+0+5+12+5+15+6+21+4+21+x$

$= 127+x$

ISBN 13 is mod 10 system. So,

$127+x$ = multiple of 10.

Immediate higher multiple of 10 to 127 is 130.

So, $127+x = 130.$

$\therefore x = 3$

Here, $x = 3$ is the check digit ~~as~~ well as missing digit.

NOTE: The last digit is called the 'check digit'.
The middle digits are called the 'missing digit'.

NOTE: Initial value of $t_1 = 0$ and $t_2 = 1$
Euclidean Algorithm is used for gcd purpose only, as well as for multiplicative inverse as well.

* Euclidean Algorithm / Multiplicative Inverse

Q.1. Find multiplicative inverse of 23 in Z_{100}.

Soln:- To find: $x \equiv \frac{1}{23} \bmod 100$

i.e. $\gcd(100, 23) = 1$

q	r_1	r_2	$r = r_1 - r_2 * q$	t_1	t_2	$t = t_1 - t_2 * q$
4	100	23	8	0	1	-4
2	23	8	7	1	-4	9
1	8	7	1	-4	9	-13
7	7	1	0	9	-13	100
	1	0	x	-13	100	x

$\gcd(100, 23) = 1$; $x = -13$

but x cannot be negative.

So, $-13 \bmod 100 = 87$

$\therefore x = 87$

$\therefore 87 \equiv (23)^{-1} \bmod 100.$

Q.2. Find x in $x \equiv \frac{-3}{13} \bmod 7$.

Soln:- $x \equiv \frac{-3}{13} \bmod 7 \Rightarrow x \equiv -3 \left[\frac{1}{13} \bmod 7\right]$

i.e. $\gcd(7, 13) = 1$

q	r_1	r_2	$r = r_1 - r_2 * q$	t_1	t_2	$t = t_1 - t_2 * q$
0	7	13	7	0	1	
1	13	7	6	1	0	
1	7	6	1	0	1	
6	6	1	0	1	-1	
	1	0	x	-1	7	

$\gcd(7, 13) = 1$; $x = -1$

Also, $x \equiv -3(-1)$

$\therefore x = 3$

$\therefore 3 \equiv \frac{-3}{13} \bmod 7$

NOTE: Initial values of $t_1 = 0$ and $t_2 = 1$
Initial values of $s_1 = 1$ and $s_2 = 0$.

_/_/___

* Extended Euclidean Algorithm.

Q.1. Find gcd(a,b), s and t for a = 161, b = 28.

Soln:- gcd(161, 28) = ?

q	r_1	r_2	$r = r_1 - r_2 * q$	s_1	s_2	$s = s_1 - s_2 * q$	t_1	t_2	$t = t_1 - t_2 * q$
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0	×	-1	4	×	6	-23	×

$\therefore$ gcd(161, 28) = 7

$s = s_1 = -1$ $\quad$ $t = t_1 = 6$

proof: gcd(161, 28) = s * a + t * b

= -1 * 161 + 6 * 28

= -161 + 168 = 7

Note: Only works if $\gcd(n_1, n_2, n_3) = 1$.

mod n

__/__/____

* Chinese Remainder Theorem.

Q. Solve for x: $x \equiv 1 \bmod 3$

$x \equiv 3 \bmod 11$

$x \equiv 6 \bmod 17$

Soln: $x \equiv 1 \bmod 3$; $a_1 = 1$; $m_1 = 3$

$x \equiv 3 \bmod 11$; $a_2 = 3$; $m_2 = 11$

$x \equiv 6 \bmod 17$; $a_3 = 6$; $m_3 = 17$

Here, $M = m_1 \times m_2 \times m_3 = 3 \times 11 \times 17 = 561$

$M_1 = \frac{M}{m_1} = \frac{561}{3} = 187$; $M_2 = \frac{561}{11} = 51$; $M_3 = \frac{561}{17} = 33$

Eucledian Algorithm for Multiplicative Inverse

Needs not be showed in exam for Chinese Remainder Theorem related questions

$M_1^{-1} \equiv 187^{-1} \bmod 3$; $M_2^{-1} \equiv 51^{-1} \bmod 11$; $M_3^{-1} \equiv 33^{-1} \bmod 17$

q	r_1	r_2	r	t_1	t_2	t
0	3	187	3	0	1	0
62	187	3	1	1	0	1
3	3	1	0	0	1	-3
	1	0	×	1	-3	×

$\therefore M_1^{-1} = 1$

q	r_1	r_2	r	t_1	t_2	t
0	11	51	11	0	1	0
4	51	11	7	1	0	1
1	11	7	4	0	1	-1
1	7	4	3	1	-1	2
1	4	3	1	-1	2	-3
3	3	1	0	2	-3	11
	1	0	×	-3	11	×

$M_2^{-1} = -3$

but it cannot be -ve

so, $M_2^{-1} = -3 \bmod 11$

$\therefore M_2^{-1} = 8$

q	r_1	r_2	r	t_1	t_2	t
0	11	33	17	0	1	0
1	33	17	16	1	0	1
1	17	16	1	0	1	-1
16	16	1	0	1	-1	17
	1	0	×	1	17	×

$M_3^{-1} = -1$

it cannot be -ve

so,

$M_3^{-1} = -1 \bmod 17$

$\therefore M_3^{-1} = 16$

So,

$$x = [(a_1 M_1 \cdot M_1^{-1}) + (a_2 \cdot M_2 \cdot M_2^{-1}) + (a_3 M_3 \cdot M_3^{-1})] \bmod M$$

$$= [187 + 1224 + 3168] \bmod 561$$

$$= 4579 \bmod 561$$

$\therefore x = 91$

__/__/____

* Caesar Cipher:

Crypt: Shift each letter ~~forward~~ three letters forward.

Decrypt: Shift each letter three letters backward.

$$f(p) = (p+3) \bmod 26.$$

Q. Produce secret message for 'PARK' using Caesar cipher.

→ P + 3 → S

A + 3 → D

R + 3 → U ∴ PARK → SDUN.

K + 3 → N

Q. What is plain message if Caesar encrypted cipher text is 'WKH'?

→ W - 3 = T

K - 3 = H ∴ WKH → THE

H - 3 = E

× —— × —— × ——— ×

Chinese Remainder Theorem → Euclidian Easier way:

$M_1^{-1} \equiv 187^{-1} \bmod 3$

means,

$187\,M_1^{-1} \equiv 1 \bmod 3$

ie, $187\,M_1^{-1} \bmod 3 = 1$

for what value of M_1^{-1}, when multiplied with 187 the remainder will be 1 when divided by 3?

$3 \times 62 = 186$; $187 - 186 = 1$

ie, $187 \times 1 - 186 = 1$

So, $M_1^{-1} = 1$.

$M_2^{-1} \equiv 51^{-1} \bmod 11$

ie, $51\,M_2^{-1} \bmod 11 = 1$

So, $51 \times ? - 11 \text{ multiples} = 1$

$51 \times 1 - (11 \times 4 \to 44) = 7\times$

$(51 \times 2)_{102} - (11 \times 9)_{99} = 3\times$

⋮

$(51 \times 8)_{408} - (11 \times 37)_{407} = 1$ ✓

∴ $M_2^{-1} = 8$

$M_3^{-1} \equiv 33^{-1} \bmod 17$

ie, $33\,M_3^{-1} \bmod 17 = 1$

So, $33 \times ? - 17 \text{ multiple}$

~~66~~ 34

~~99~~ 51

~~132~~ 68

165 85

⋮ 102

495 ~~493~~

528 - 527

$33 \times 16 = 528$

$\therefore M_3^{-1} = 16$

_/_/____

* RSA (Rivest Shamir Adleman) Cryptosystem.

Q. $p=23$. $q=31$. $e=83$. Compute d. Convert 'CSE' to cipher-text using ASCII Codes (67, 83, 69). Convert back to plaintext as well.

Sol'n:

$p=23$; $q=31$. So, $n = p \times q = 23 \times 31 = 713$

and, $\phi(n) = (p-1) \times (q-1) = 660$.

$e = 83$ (given)

IF e was not given (if) and we had to calculate e by ourselves, then, e is such that $1 < e < \phi(n)$

and $\gcd(\phi(n), e) = 1$.

So, e could be anything between 1 to 660 and $\gcd(660, e) = 1$.

For instance, e can be selected as 7, 13, 17, 19, ...

i.e, any co-primes would work.

Now, $d \equiv e^{-1} \bmod \phi(n)$

i.e., $de \equiv \bmod \phi(n)$ or, $de \bmod \phi(n) = 1$.

So, $83d \bmod 660 = 1$

i.e., $83 \times ? - \text{multiples of } 660 = 1$

$83 \times 8 = 664 \quad - \quad 660 \times 1 = 660 \quad = 4\checkmark$

Accordingly, $83 \times 16 = 1328 - 660 \times 2 = 1320 \quad = 8\checkmark$

....

OR FROM EUCLEDIAN ALGORITHM

q	r_1	r_2	r	t_1	t_2	t
7	660	83	79	0	1	-7
1	83	79	4	1	-7	8
19	79	4	3	-7	8	-159
1	4	3	1	8	-159	167
3	3	1	0	-159	167	-660
	1	0	x	167	-660	

__/__/____

$\therefore d = 167.$

$83 \times 167 - 660 \times 21 = 1$
$\therefore 13861 - 13860 = 1$ ✓

Now,

Public key, $KU = \{e, n\} = \{83, 713\}$
Private key, $KR = \{d, n\} = \{167, 713\}$

For Encryption,

$C = M^e \bmod n$; M is plaintext & $M < n$

So, for ascii CSE, $M = 67, 83, 69$.

for $M = 67$; $C = 67^{83} \bmod 713$

$= [(67^2)^{41} \times 67] \bmod 713$

$= [(211^2)^{20} \times 211 \times 67] \bmod 713$

$= [((315)^2)^{10} \times 590] \bmod 713$

$= [((118)^2)^5 \times 590] \bmod 713$

$= [((377)^2)^2 \times 377 \times 590] \bmod 713$

$= [(242)^2 \times 687] \bmod 713$

$= 40233468 \bmod 713$

$\therefore C = 304$

for $M = 83$; $C = 83^{83} \bmod 713$

$\therefore C = \ldots$ (Let's say C_2)

for $M = 69$, $C = 69^{83} \bmod 713$

$\therefore C = \ldots$ (Let's say C_3)

So, the values of $C = 304, C_2, C_3$ are then converted to corresponding ASCII values and then, inplace of plaintent 'CSE', the encrypted ASCII characters for $304, C_2, C_3$ are sent.

for decryption, ASCII characters are converted to ASCII values which will be $304, C_2, C_3$.

For decryption,

$M = C^d \pmod n$; C is cyphertext.

Here, Cyphestexts comesponding values,

$C = 304, C_2, C_3$

for $C = 304$, $M = 304^{167} \bmod 713$

$= (304^2)^{83} \times 304 \bmod 713$

$= (439^2)^{41} \times 304 \times 439 \bmod 713$

$= ((211)^2)^{20} \times 211 \times 125 \bmod 713$

$= (315^2)^{10} \times 707 \bmod 713$

$= (118^2)^5 \times 707 \bmod 713$

$= ((377)^2)^2 \times 377 \times 707 \bmod 713$

$= 242^2 \times 590 \bmod 713$

$= 98 \times 590 \bmod 713$

$\therefore M = 67$

Similarly, for $C = C_2$, $M = C_2^{167} \bmod 713$

$\therefore M = 83$

And for $C = C_3$, $M = C_3^{167} \bmod 713$

$M = 69$

The decrypted plaintexts ~~have~~ are $M = 67, 83, 69$ from ASCII reference, when these three values are converted, we get plaintext CSE

NOTE: Conversion code can be anything - ASCII code or maybe even just A=1, B=2 ... Z=26 code or any specified.

* Deffie-Hellman Key Agreement Protocol.

Q. Alice and Bob agree to use prime $p = 11$. Find primitive root g. Alice chooses private key $x = 4$ and Bob chooses his private key $y = 5$ (private key < prime). Calculate public keys for both Alice and Bob. Then finally calculate secret keys k_1 and k_2 and show $k_1 = k_2$. [Secret keys must always be equal/same]

Soln:-

prime, $p = 11$.

Primitive root $g = 2$ ∵ [illegible]

$2^1 \bmod 11 = 2$;
$2^2 \bmod 11 = 4$;
$2^3 \bmod 11 = 8$;
$2^4 \bmod 11 = 5$;
$2^5 \bmod 11 = 10$;
$2^6 \bmod 11 = 9$;
$2^7 \bmod 11 = 7$;
$2^8 \bmod 11 = 3$
$2^9 \bmod 11 = 6$
$2^{10} \bmod 11 = 1$

How to find primitive root, g ?

If $g \bmod p$, $g^2 \bmod p$, ... $g^{p-1} \bmod p$ give results $\{1, 2, 3, \ldots p-1\}$ then, p is primitive.

i.e, results are $= \{2,4,8,5,10,9,7,3,6,1\} = \{1,2,3,4,5,6,7,8,9,10\}$

Now,

Alice (Private key, $x = 4 < 11$)	Bob (Private key, $y = 5 < 11$)
Public key, $S_A = g^x \bmod p$ $S_A = 2^4 \bmod 11$ $\therefore S_A = 5$	Public key, $S_B = g^y \bmod p$ $S_B = 2^5 \bmod 11$ $\therefore S_B = 10$
Secret key, $K_1 = (S_B)^x \bmod p$ $= (10)^4 \bmod 11$ $\therefore K_1 = 1$	Secret key, $K_2 = (S_A)^y \bmod p$ $= 5^5 \bmod 11$ $\therefore K_2 = 1$

$\therefore K_1 = K_2$.

i.e, exchange is successful.

__/__/____

* RSA Digital Signature Scheme

Q. M=8. Find S in the Sender side. Verify the message M and the signature received in the receiver side.

Soln;

Let, $p = 7$; $q = 11$

$n = p * q = 7 \times 11 = 77$

$\phi(n) = (p-1)(q-1) = 6 \times 10 = 60.$

Choosing, $e = 13$ $\quad (1 < e < n ;\ \gcd(\phi(n), e) = 1)$

$d \equiv e^{-1} \bmod \phi(n)$

Or, $13d \equiv 1 \bmod 60$

$\therefore 13 \times 37 \equiv 1 \bmod 60 \quad (\times 8)$

$\therefore d = 37$

Finding S, in Sender's Side

$S = M^d \bmod n$

$= 8^{37} \bmod 77$

$= (8^3)^{12}\ 8 \bmod 77$

$= (50^3)^4\ 8 \bmod 77$

$= 29^4 \times 8 \bmod 77$

$= 36 \times 8 \bmod 77$

$\therefore S = 57$

Verifying M', in Receiver's side

$M' = S^e \bmod n$

$= 57^{13} \bmod 77$

$= (57^2)^6 \cdot 57 \bmod 77$

$= 15^6 \cdot 57 \bmod 77$

$\therefore M' = 15 \cdot 57 \bmod 77 = 8$

Since, $M = M'$; message/signature is verified.

__/__/____

* CRC - Cyclic Redundancy Check

→ Given divident (also called WORD) and divisor either directly in binary form or in polynomial.

Let's say: Divident is given : 1010101010
and divisor is given: $x^4 + x^3 + 1$

→ Convert both divident and divisor to binary

Divident = 1010101010

Divisor = $\underbrace{1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x^1 + 1 \cdot x^0}$

11001 is the divisor

→ Now, Add (or Append) redudency bits to divident, i.e.,
no. of bits of divisor - 1 zeros.
i.e, here, 11001 is 5 bits so, 5 - 1 = 4
So, 4 zeros will be added to divident making it, 10101010100000

→ Let's divide,

```
11001 ) 10101010100000
        11001
        -----
        011000
         11001
        -----
         00001000
             11001
             -----
             00011000
                11001
                -----
                000010   ← Remainder
```

No need to write quotients
We will XOR instead of subtract.

fill redundancy zeros with last four (bit-1) digits.
i.e, Receiver will get code → 10101010100010

This is main aim of CRC to check if error is present.
{ To check if the received code has error or not, divide it in the same way with divisor. If
remainder = 0 ; then no error.
remainder ≠ 0 ; then some error is present

__/__/____

* HAMMING CODE : error detection & correction.

→ Parity Bits : Denoted by P_n

→ Data Bits : Denoted by D_n

→ Parity Bits are present at $n=2^0, 2^1, 2^2 \ldots$ places.

for 7 bit code, | D_7 | D_6 | D_5 | P_4 | D_3 | P_2 | P_1 |

Also, P_1 is associated with, $P_1 \rightarrow D_3 D_5 D_7$

P_2 is associated with, $P_2 \rightarrow D_3 D_6 D_7$

P_4 is associated with, $P_4 \rightarrow D_5 D_6 D_7$

→ If even parity, $P_1 D_3 D_5 D_7$; $P_2 D_3 D_6 D_7$; $P_4 D_5 D_6 D_7$ should resemble binary form having even ones.

→ If odd parity, $P_1 D_3 D_5 D_7$; . . . . . should resemble binary form having odd ones.

Example: Detecting Error, if PDDD → ☐☐☐☐ should be even parity but are odd OR should be odd parity but are even, in these error cases, $P_n = 1$ and if no error, then $P_n = 0$

Which bit has error? E = | P_{n_3} | P_{n_2} | P_{n_1} |

Convert it to decimal. That place has error

EXAMPLE:

Check and correct error for 1011011 assuming even parity.

1	0	1	1	0	1	1
D_7	D_6	D_5	P_4	D_3	P_2	P_1

$P_1 D_3 D_5 D_7 = 1011$ (odd, so error) $\therefore P_1 = 1$

$P_2 D_3 D_6 D_7 = 1001$ (even, no error) $\therefore P_2 = 0$

$P_4 D_5 D_6 D_7 = 1101$ (odd, so error) $\therefore P_4 = 1$

P_4	P_2	P_1
1	0	1

$(101)_{20}$

$\hookrightarrow (5)_{10}$

that means 5th place has error. So the correct code is 1001011

SET THEORY: __/__/____

* **Set:** A set is any well defined collection of objects (called the elements or members of the set).

NOTATION: Capital letters A, B, C... denote sets
Lowercase letters a, b, c... denote elements of sets.

$$A = \{a, b, c\}$$

$N \rightarrow$ Natural Numbers $\{1, 2, 3...\}$; $Z \Rightarrow$ Integers $\{-\infty ... -1, 0, 1, ... \infty\}$
$R \rightarrow$ Real Numbers ; ~~$R \neq$ Real No.~~
$Q \rightarrow$ Rational Numbers $\{\frac{p}{q} \text{ form}\}$; $C \rightarrow$ Complex No.

* Representation of sets:

(Roster) Tabular form: $A = \{1, 4, 9, 16\}$

Set Builder form (Rule method): $A = \{x : x = n^2 \text{ and } 1 \leq n \leq 4, n \in N\}$

* Set Operations:

1. Every set exists within some universe U. i.e., $A = \{a \in U\}$
2. Complement: $A' = \{a \in U \mid a \notin A\}$
3. Intersection: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
4. Union: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
5. Difference: $A - B = \{x \mid x \in A \text{ and } x \notin B\}$
6. ~~Empty Sets~~ $= A \cap \bar{B}$

* Cardinality of Set:

Cardinality of set A is number of elements in A, which is written as $|A|$.

E.g.: $|\{2, 6, 7\}| = 3$

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

$|\{\}| = 0 = |\phi|$; $|\{\phi\}| = 1$

$|\{\{1, 2\}, \{3, 4\}\}| = 2$

* Power Set:

for Set S, power set is the set of all subsets of S.

for set $S = \{0, 1, 2\}$

$P(S) = P(\{0,1,2\}) = \{\phi, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\}$

$P(\phi) = \{\phi\}$ ⟶ Empty Set

$P(\{\phi\}) = \{\phi, \{\phi\}\}$ ⟶ singleton set.

* Cartesian Product.

$A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$

E.g.: $A = \{1,2\}$, $B = \{a,b,c\}$,

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

→ Unless $A = \phi$ or $B = \phi$, Cartesian Products $A \times B$ and $B \times A$ are not equal. $A \times B \neq B \times A$

→ If $A \cap B = \phi$, Disjoint Sets.

Relations (R)

* Properties of Relations:

1. Reflexive: $(a,a) \in R$, for $\forall a \in A$
2. Symmetric: $(b,a) \in R$ whenever $(a,b) \in R$, $\forall a,b \in A$
3. Antisymmetric: $\forall a,b \in A$, if $(a,b) \in R$ and $(b,a) \in R$; $a = b$
4. Transitive: $(a,b) \in R$ and $(b,c) \in R$ then $(a,c) \in R$, $\forall a,b,c \in A$

* Composition of Relations.

for $A = \{1, 2, 3\}$

$B = \{p, q, r\}$

$C = \{x, y, z\}$

Given, $R = \{(1,p), (1,r), (2,p), (2,q)\}$

$S = \{(p,y), (q,x), (q,y), (r,z)\}$

Then, Composition of R and S,

$S \circ R = \{(1,y), (1,z), (2,y), (2,x), (2,y)\}$

$= \{(1,y), (1,z), (2,y), (2,x)\}$

i.e, $a \in A, b \in B, c \in C$; $(a,b) \in R$, $(b,c) \in S$

Then, $S \circ R = \{(a,c)\}$

* Representation of Relations:

(i) Using Matrix

(ii) Using Digraphs

__/__/____

* Matrix Representation of Relations:

Let $A = \{a_1, a_2, \ldots, a_m\}$

$B = \{b_1, b_2, \ldots, b_n\}$

Then,

Matrix of R, $M_R = [m_{ij}]$, where $m_{ij} = \begin{cases} 1, & \text{if } (a_i, b_j) \in R \\ 0, & \text{if } (a_i, b_j) \notin R \end{cases}$

i.e.,

$$\begin{array}{c} \\ a_1 \\ a_2 \\ \vdots \\ a_m \end{array} \begin{array}{c} \begin{array}{cccc} b_1 & b_2 & \cdots & b_n \end{array} \\ \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1n} \\ m_{21} & m_{22} & \cdots & m_{2n} \\ \vdots & \vdots & & \vdots \\ m_{m1} & m_{m2} & \cdots & m_{mn} \end{bmatrix}_{m \times n} \end{array}$$

E.g.: $A = \{1, 3, 4\}$, $B = \{1, 3, 4\}$

$R = \{(1,1), (1,3), (3,3), (4,4)\}$

Then $M_R =$

	1	3	4
1	1	1	0
3	0	1	0
4	0	0	1

* Properties. (x is don't care, either 0 or 1; any)

1. **Reflexive.** $m_{ii} = 1$ (diagonal 1)

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

2. **Irreflexive:** $m_{ii} = 0$ (diagonal 0)

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

3. **Symmetric:** $m_{ij} = m_{ji}$

$$\text{eg.} \rightarrow \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

4. **Antisymmetric:** $m_{ij} = 1$, $m_{ji} = 0$

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \leftarrow \text{e.g.:}$$

5. **Asymmetric:** $m_{ii} = 0$, $\{m_{ij} = 1, m_{ji} = 0$ / $\{m_{ji} = 1, m_{ij} = 0$

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

6. **Transitive:** $m_{ij} = 1$; $m_{jk} = 1 \Rightarrow m_{ik} = 1$

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

= arrows are

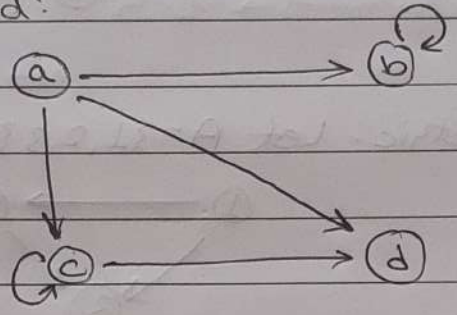
__/__/____

* Graph Representation of Relations:

Let $A = \{a, b, c\}$, $B = \{b, c, d\}$; $R \subseteq A \times B$

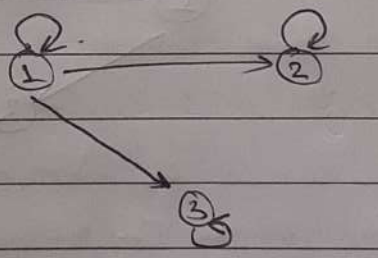
$R = \{(a,b), (a,c), (a,d), (b,b), (c,c), (c,d)\}$

Graph is so formed:



* Properties:

1. Reflexive: Let $A = \{1,2,3\}$; $R = \{(1,1), (2,2), (3,3), (1,2), (1,3)\}$

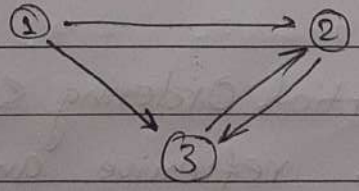


Self loop is ~~must~~ for reflexive.

(x,x) (x,x)

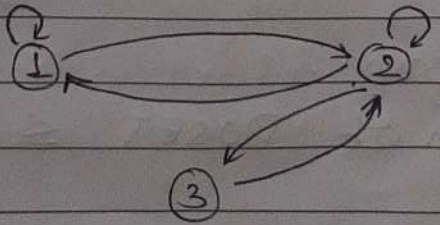
x is dont care

2. Irreflexive. Let $A = \{1,2,3\}$; $R = \{(1,2), (2,3), (1,3), (3,2)\}$



No self loops.

3. Symmetric: Let $A = \{1,2,3\}$; $R = \{(1,1), (1,2), (2,1), (2,3), (3,2), (2,2)\}$

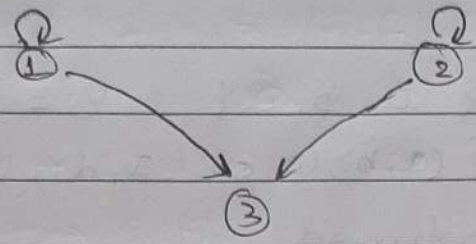


~~Every~~ closed loop between two vertex

① ② are vertices. ⇌ arrows are edges

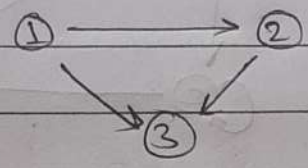
__/__/____

4. Antisymmetric: Let $A=\{1,2,3\}$; $R=\{(1,1),(2,2),(2,3),(1,3)\}$



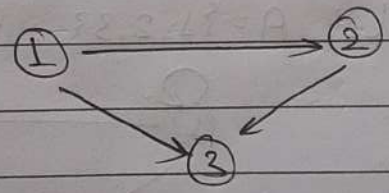
No closed loop

5. Asymmetric: Let $A=\{1,2,3\}$; $R=\{(1,2),(2,3),(1,3)\}$



No self loop
No closed loop.

6. Transitive: Let $\{1,2,3\}=A$. $R=\{(1,2),(2,3),(1,3)\}$



ie,
if $1 \to 2$
and $2 \to 3$
then
$1 \to 3$ must.

* Equivalence Relation:
If relation is all symmetric, reflexive and transitive.

* POSET (Partial Ordering Set):
If relation is reflexive, antisymmetric and transitive.
E.g.: Partial Order $\leq$ or $\geq$
i.e, if $a \geq b \geq c$; it is poset.

* Hasse Diagram.
Representation of POSET $\leq$ is called Hasse diagram
$(X, \leq)$

$\leq$ is relation

$\leq$ can be anything, like ~~not~~ divide, less than equal to, subset $\subseteq$.

__/__/____

divide

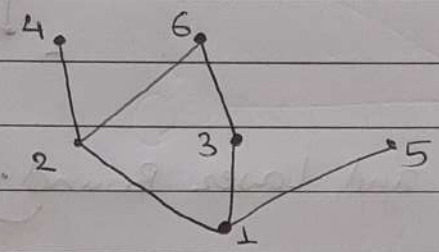
Eg.: Let $X = \{1, 2, 3, 4, 5, 6\}$. '/' is partial order relation

So, $R = \{(1,2), (1,3), (1,4), (1,5), (1,6), (2,4), (2,6), (3,6)\}$

Transitive — Transitive

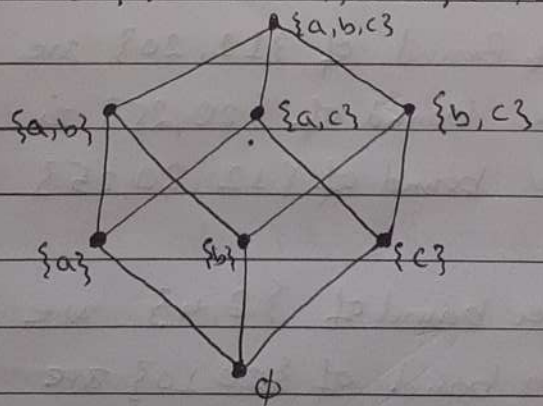
POSET will be $\{(1,2), (1,3), (1,4), (1,5), (1,6), (2,4), (2,6), (3,6)\}$

Hasse Diagram will be,



Example 2: Hasse diagram for POSET $(P(S), \subseteq)$, where $P(S)$ is power set on $S = \{a, b, c\}$

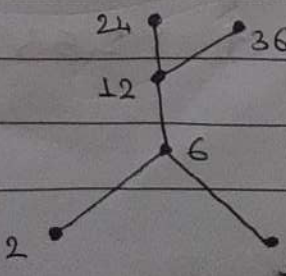
Solⁿ:- $P(S) = \{\phi, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$



Example 3: $X = \{2, 3, 6, 12, 24, 36\}$ relation $\leq$ such $x \leq y$ if x divides y.

$R = \{(2,6), (2,12), (2,24), (2,36), (3,6), (3,12), (3,24), (3,36), (6,12) \ldots\}$

POSET $= \{(2,36), (3,36), (6,36), (12,36)\}$



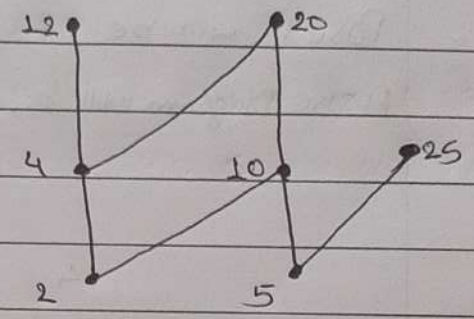
__/__/____

* Maximal and minimal.

E.g: Poset ({2, 4, 5, 10, 12, 20, 25}, |)

Maximal elements → 12, 20, 25

Minimal elements → 2, 5



* Upper Bound and Lower Bound.

In above,

Upper Bound of {2, 5} are 10, 20

No lower Bound of {2, 5}.

Lower Bound of {12, 20} are 4, 2

Lower bound of {20, 25} is 5.

Lower bound of {12, 20, 25} none.

Upper bound of {2, 4} are 4, 12, 20.

Lower bound of {20, 10} are 10, 2, 5

* Greatest lower bound and least Upper Bound.

Greatest LB of {20, 10} is 10

Greatest LB of {12, 20} is 4

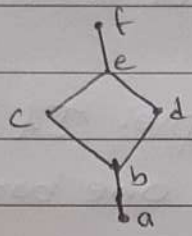
Lowest UB of {2, 4} is 4

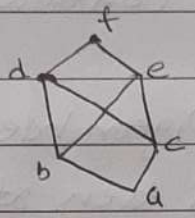
Lowest UB of {2, 5} is 10

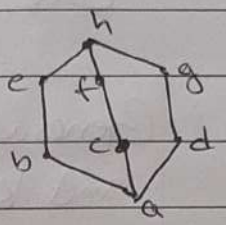
__/__/____

* Lattices: Poset in which every pair of elements has both a least upper bound and greatest lower bound.

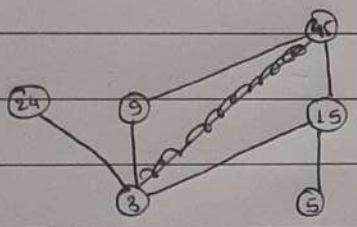
E.g:







Q.



Find, maximal elements,
minimal elements,
greatest element.
~~least element~~.
Upper bound of {3,5}
least upper bound of {3,5}, if exists
lower bound of {15,45}
Greatest lower B. of {15,45}, if exi

Ans: Maximal elements: 24, 45
Minimal elements: 3, 5
Upper bounds of {3,5} = 15, 45
Least UB of {3,5} = 15
Lower bounds of {15,45} = 15, 3, 5
Greatest LB of {15,45} = 15

Elementary Combinatories

_/_/____

* Pigeonhole Principle: If there are n boxes and n+1 objects or more objects, then at least one box contains 2 or more objects.

* Generalised Pigeonhole principle: If there are N objects and K boxes, then at least one box contains [N/K] objects.