No. 1

Date : / /

Q.1.

Ans If $a^3 | b^2$ then $a | b$

$b^2 = a^3 K \qquad K \in Z$

$\frac{b^2}{a^2} = aK$

$b/a = \sqrt{aK}$

↓

Rational To prove $a|b$. we need to show b/a is an integer.

Now $a \times K$ is an integer.

It's square root can be integer or irrational.

If it's irrational & we know that b/a is rational so Irrational = Rational which is not true.

So square root must be integer.

Hence b/a must be integer.

so $a|b$.

No. (2)
Date : / /

Q.2.

Ans. Given $q \mid 2^p - 1$

To prove $p < q$.

$2^p \equiv 1 \bmod q$ (from question) - (1)

$2^{q-1} \equiv 1 \bmod q$ from Fermat's little Theorem - (2)

From (1) & (2)

$2^{q-1} \equiv 2^p \pmod q$

$2^{q-1}(1 - 2^{p+1-q}) \equiv 0 \bmod q$

Either $2^{q-1} \equiv 0 \bmod q$.

or $(1^0 - 2^{p+1-q}) \equiv 0 \bmod q$.

Using theorem

If $a \equiv a' \bmod n$ & $b \equiv b' \bmod n$

$\Rightarrow a \cdot b \equiv a' \cdot b' \pmod n$

But $2^{q-1} \equiv 0 \bmod q$

is not possible for any value of q.

So $(1 - 2^{p+1-q}) \equiv 0 \bmod q$

or $(2^{q-p-1} - 1) \equiv 0 \bmod q$

power of 2 must be greater than or equal to zero.
If power of 2 is negative number will be formed fraction
∴ Here modulo 0 is not possible.

So $q - p - 1 \geq 0$

$q \geq p + 1$

$q > p$

Hence $p < q$ proved.

Q.3.
Ans.

$n > 1$ is an odd integer

$\phi(2n) = \phi(n)$

$\phi(mn) = \phi(m)\,\phi(n)$

since $\gcd(m, n) = 1$

Here $m = 2$ $n = n$ and n is odd

So $\gcd(2, n) = 1$

$\phi(2n) = \phi(2) \cdot \phi(n)$ $\quad \phi(2) = 1$

$\phi(2n) = 1 \cdot \phi(n)$

$\phi(2n) = \phi(n)$

proved.

No. 4

Date : / /

Q.4.

$2a-1 \mid a^2+2$ given.

let $\frac{a^2+2}{2a-1} = K$ — (1) $K \in Z$

multiply both sides by 4.

$4\left[\frac{(a^2+2)}{2a-1}\right] = 4k = m \quad m \in Z$

$\frac{4a^2+8}{2a-1}$

$\frac{(2a-1)^2 + 4a + 7}{2a-1} = m$

$2a-1 + \frac{4a+7}{2a-1} = m$

$\downarrow$ integer. $\frac{4a+7}{2a-1}$ also needs to be integer

$\Rightarrow \frac{4a+7}{2a-1} \Rightarrow \frac{4a-2+9}{2a-1}$

$\Rightarrow \frac{2(2a-1)+9}{2a-1}$

$\Rightarrow 2 + \frac{9}{2a-1} = k \quad k \in Z$

No. 5

Date : / /

$\frac{9}{2a-1}$ must be integer

$2a-1$ can take values from $\pm 1, \pm 3, \pm 9$.

$2a-1=1$ $\quad$ $2a-1=-1$ $\quad$ $2a-1=3$

$a=1$ $\quad$ $a=0$ $\quad$ $2a=4$

$a=2$

$2a-1=-3$ $\quad$ $2a-1=9$ $\quad$ $2a-1=-9$

$2a=-2$ $\quad$ $2a=10$ $\quad$ $2a=-8$

$a=-1$ $\quad$ $a=5$ $\quad$ $a=-4$

$a \in \{1, 0, -1, 5, 2, -4\}$

checking each value in question

(1) $\frac{a^2+2}{2a-1} \Rightarrow \frac{3}{1} = 3 \quad 3 \in \mathbb{Z}$

(2) $\frac{a^2+2}{2a-1} \Rightarrow \frac{(0)^2+2}{2(0)-1} = \frac{2}{-1} = -2 \in \mathbb{Z}$

(3) $\frac{a^2+2}{2a-1} \Rightarrow \frac{(-1)^2+2}{2(-1)-1} = \frac{3}{-3} = -1 \in \mathbb{Z}$

(4) $\frac{a^2+2}{2a-1} \Rightarrow \frac{(5)^2+2}{2(5)-1} = \frac{27}{9} = 3 \in \mathbb{Z}$

(5) $\frac{(2)^2+2}{2(2)-1} \Rightarrow 6/3 = 2 \in \mathbb{Z}$

(6) $\frac{(-4)^2+2}{2(-4)+1} \Rightarrow \frac{18}{-9} = -2 \in \mathbb{Z}$

So possible values of a are $\{1, 0, -1, 5, 2, -4\}$

Q.5.
Ans.

$$\frac{a^n-1}{a-1} = a^{n-1} + a^{n-2} + a^{n-3} + \ldots 1$$

$$\Rightarrow 1^{n-1} + 1^{n-2} + \ldots 1 = n \bmod (a-1)$$

$$\gcd\left(\frac{a^n-1}{a-1}, a-1\right) = \gcd(n, a-1)$$

Q.6.
Ans.

Let us assume $\sqrt{p}$ is rational.
So $\sqrt{p}$ can be represented in the form of a/b. where $a, b \in \mathbb{Z}$ and $b \neq 0$.

$$\sqrt{p} = \frac{a}{b}$$

$$p = \frac{a^2}{b^2} \qquad b^2 = \frac{a^2}{p}$$

$\Rightarrow a^2$ is divisible by p
$\Rightarrow a$ is divisible by p

$a = pm$ for $m \in \mathbb{Z}$.

$a^2 = p^2 m^2$

$\Rightarrow b^2 p^2 = p^2 m^2$

$\Rightarrow b^2 = pm^2$

$\Rightarrow b^2$ is divisible by p
$\Rightarrow b$ is divisible by p.

$\Rightarrow p$ divides both a & b.
$\Rightarrow a$ & b have p as one common factor.

But we know that a & b are coprime.
This contradicts our initial assumption
$\sqrt{p}$ is rational
So $\sqrt{p}$ is irrational.

Q.7.
Ans.

$42x \equiv 12 \bmod 90 \quad = \quad ax = b \bmod m$

$\gcd(42, 90) = 6 = d$

Here $d \mid b$ is zero.
So it must have d solutions.

So trying all possibles from 0 to 11.

$42(0) \bmod 90 = 0 \neq 12$

$42(1) \bmod 90 = 42 \neq 12$

$42(2) \bmod 90 = 84 \neq 12$

$42(3) \bmod 90 = 36 \neq 12$

$42(4) \bmod 90 = 78 \neq 12$

$42(5) \bmod 90 = 30 \neq 12$

$42(6) \bmod 90 = 72 \neq 12$

$42(7) \bmod 90 = 24 \neq 12$

$42(8) \bmod 90 = 66 \neq 12$

$42(9) \bmod 90 = 18 \neq 12$

$42(10) \bmod 90 = 60 \neq 12$

$42(11) \bmod 90 = 12 = 12$

So $x = 11$ is one solution.

other solutions can be generated directly.

$$11 + \frac{90}{\gcd(42,90)} * K \qquad K \in \mathbb{Z}$$

$$11 + 15 * K$$

$K = 0 \quad x = 11$

$K = 1 \quad x = 26$

$K = 2 \quad x = 41$

$K = 3 \quad x = 56$

$K = 4 \quad x = 71$

$K = 5 \quad x = 86$

So $x = \{11, 26, 41, 56, 71, 86\}$

No. 9
Date : 4/1

Q.9.
Ans.

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{84}$$

$$\frac{x+y}{xy}=\frac{1}{84}$$

$$xy-84(x+y)=0$$

adding 84^2 both sides.

$$xy-84(x+y)+84^2=84^2$$

$$(x-84)(y-84)=84^2$$

let $x-84=a$ & $y-84=b$

$$a\times b=84^2$$

No of solutions possible are factors of 84^2

$$84^2=2^4\times3^2\times7^2$$

$$\Rightarrow (4+1)(2+1)(2+1)$$
$$\Rightarrow 5\times3\times3$$
$$\Rightarrow 45$$

So 45, ordered pair are possible.

No. 10
Date : / /

Q.8. $\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$

$$\frac{x+y}{xy} = \frac{1}{n}$$

$$xy - n(x+y) = 0$$

adding n^2 both sides

$$xy - n(x+y) + n^2 = n^2$$

$$(x-n)(y-n) = n^2$$

let $x-n = a$ & $y-n = b$

So $a * b = n^2$

No of solutions = are possible factors of n^2

$$n^2 = (p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_m^{\alpha_m})^2$$

$$\Rightarrow p_1^{2\alpha_1} * p_2^{2\alpha_2} * p_3^{2\alpha_3} * p_m^{2\alpha_m}.$$

$p_i \in$ prime

$\alpha_i \in$ integers

so,

solutions

$(2\alpha_1+1)(2\alpha_2+1) \cdots (2\alpha_m+1)$

ordered pair are possible.

Q.10.

Ans.

$x \equiv 3 \bmod 7$

$x \equiv 11 \bmod 18$

$x \equiv 5 \bmod 24$

$x \equiv 3 \bmod 7$

$x \equiv 11 \bmod 9$

$x \equiv 11 \bmod 2$

$x \equiv 5 \bmod 8$

$x \equiv 5 \bmod 3$

① $x \equiv 11 \bmod 9$ $x = \{2, 11, 20 \ldots\}$

$x \equiv 5 \bmod 3$ $\{x = 5, 8, 11, 14, 17, 20$

Here $x \equiv 11 \bmod 9$ is having higher power of 3.
So lower can be ignored

② $x \equiv 11 \bmod 2$ 2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21..

$x \equiv 5 \bmod 8$ 5, 13, 21, ...

Both congruences for powers of 2 are implied by the congruence with the higher power.
So lower ignored.

No. 12

Date : / /

$x \equiv 3 \bmod 7$

$x \equiv 11 \bmod 9$

$x \equiv 5 \bmod 8$

$N = m_1 m_2 * m_3$

$m_1 = 7 \quad m_2 = 9 \quad m_3 = 8$

$a_1 = 3 \quad a_2 = 11 \quad a_3 = 5$

Here m_1, m_2, m_3 are relatively coprime. So, It can be solved using CRT.

$N = 7 \times 9 * 8 = 504$

$N_1 = \frac{504}{7} = 72$

$N_2 = \frac{504}{9} = 56$

$N_3 = \frac{504}{8} = 63$

(1) $72^{-1} \bmod 7$

$\Rightarrow 72 = 10 * 7 + 2$

$7 = 3 \times 2 + 1$

$1 = 7 - 3 * 2$

$2 = 72 - 10 * 7$

$\Rightarrow 7 - 3 * (72 - 10 * 7)$

$\Rightarrow 7 - 3 \times 72 + 30 * 7$

$\Rightarrow 31 * 7 - 3 * 72$

taking mod 7 on both sides.

$-3 \times 72 = 1 \bmod 7$

$72^{-1} \bmod 7 = -3 \bmod 7 = 4$

$72^{-1} \bmod 7 = 4 = z_1$

(2) $56^{-1} \bmod 9 = z_2$

$56 = 6 * 9 + 2$

$9 = 4 * 2 + 1$

$56 - 6 \times 9 = 2$

$1 = 9 - 4 * 2$

$1 = 9 - 4 \times (56 - 6 * 9)$

$1 = 9 - 4 * 56 + 24 * 9$

$1 = 25 * 9 - 4 * 56$

taking mod 9 both sides

$1 \bmod 9 = (-4) * 56 \bmod 9$

$56^{-1} \bmod 9 = -4 \bmod 9 = 5$

$z_2 = 5$

3 = $63^7 \bmod 8 = z_3$

$63 = 7 * 8 + 7$

$8 = 1 * 7 + 1$

$7 = 63 - 7 \times 8$

$1 = 8 - 1 * 7$

$1 = 8 - 1 * (63 - 7 \times 8)$

$1 = 8 - 63 + 7 * 8$

$1 = 8 * 8 + 1 \times 63$

Taking mod 8 both sides.

$1 \bmod 8 = -1 \times 63 \bmod 8 = 1$

$63^7 \bmod 8 = 7$

Now using CRT.

$(3 * 72 * 4 + 11 * 56 \times 5 + 5 * 63 \times 7) \bmod 504$

$(864 + 3080 + 2205) \bmod 504$

$\Rightarrow 6149 \bmod 504$

$\Rightarrow x \equiv 101 \bmod 504$

Q.13

$p = 4k+1$ where p is prime number.

Using wilson's theorem.

$(p-1)! \equiv -1 \bmod p$.

$(4k+1-1)! \equiv -1 \bmod p$

$4k! \equiv -1 \bmod (4k+1)$

$4k! \equiv (4k)(4k-1)(4k-2) \cdots (2k+1) \cdots 1$

taking mod $(4k+1)$

$\equiv (-1)(-2)(-3) \cdots (-2k)(-2k-1) \cdots (-4k)$

$\equiv (-1)^{2k} (1 \cdot 2 \cdot 3 \cdots 2k-1)\, 2k)^2$

$\equiv 1 \cdot (2k)! \, (2k)!$

$1 \equiv (2k)!^2 \bmod 4k+1$

So $2k!$ is square root of -1 modulo $4k+1$

No. 16

Date : / /

Q12

$$n = \prod_{i=1}^{m} p_i$$

$$n = p_1 \times p_2 \cdots p_m$$

$$\lambda(n) = \min \{ k_i(p_i - 1) : k_i(p_i - 1) = k_1(p_1 - 1), i \in \{1, 2 \cdots m\} \}$$

This means $\lambda(n)$ is the minimum of $k_1(p_1 - 1)$ such that $k_i(p_i - 1) = k_1(p_1 - 1)$ for $i \neq 1$ for some $k_i \in \mathbb{Z}$.

$$\Downarrow$$

$$\lambda(n) = LCM \{ (p_1 - 1), (p_2 - 1)(p_3 - 1) \cdots (p_m - 1) \} \quad -(1)$$

In the question

$$n = p_1 \times p_2 \cdots p_m$$

Then using Carimcheal function

$$\lambda(n) = LCM \{ \lambda(p_1), \lambda(p_2) \cdots \lambda(p_m) \}$$

since p_i is prime for all i

$$\lambda(p_i) = \varphi(p_i)$$

No. 17
Date : / /

$\lambda(n) = LCM\{\phi(p_1), \phi(p_2) \ldots \phi(p_m)\}$

$= LCM((p_1-1), (p_2-1)(p_3-1) \ldots (p_m-1))$ — (2)

we know that

$\phi(p_i) = (p_i - 1)$ for a prime p.

from (1) & (2) we have proved.

Q.14.

C : 25 M : 17

Z : 24

A : 24

U : 24

We might C is the encryption of e and similarly Z is the encryption of t

$e_k(4) = 2$

$e_k(19) = 25$

$4a + b = 2$

$19a + b = 25$

$15a \equiv 23 \bmod 26$ — (1)

Here gcd(15, 26) = 1
So only 1 solution exist.

Finding inverse of 15 modulo 26.

$15^{-1} \bmod 26 =$

$26 = 1 \times 15 + 11$ $\quad 11 = 26 - 15$
$15 = 1 \times 11 + 4$ $\quad 4 = 15 - 11$
$11 = 2 \times 4 + 3$
$4 = 1 * 3 + 1$ $\quad 3 = 1$

$1 = 4 - 3$
$3 = 11 - 2 \times 4$

$1 = 4 - (11 - 2 * 4)$
$4 - 11 + 2 \times 4$
$1 = 3 \times 4 - 11$

$1 = 3 * (15 - 11) - 11$
$1 = 3 * 15 - 4 * 11$

$1 = 3 \times 15 - 4(26 - 15)$

$1 = 3 * 15 - 4 \times 26 + 4 \times 15$

$1 = 7 \times 15 - 4 * 26$
taking mod 26 both sides.

$1 = (7 \times 15) \bmod 26$

$15^{-1} = 7$

Now in equation (1)

Multiply both sides by 7.

$15a * 7 \equiv (23 \times 7) \bmod 26$

$a \equiv 5 \bmod 26$

$a = 5$

$4(5) + b \equiv 2 \bmod 26$

$b = 8$

$x = a^{-1}(y - b) \bmod 26$

$5^{-1} = 21$

$x = 21(y - 8) \bmod 26$

$x = (21y - 12) \bmod 26$

ZRC

$z = 25 = y$

$(21 \times 25 - 12) \bmod 26 = 19$

$19 = 19 = T$

$R = 17 = y$

$(21 \times 17 - 12) \bmod 26 = 7$

$7 = H$

Decrypted text is:

THE ART OF WRITING SECRET MESSAGES WHICH IS INTELLIGIBLE TO THOSE WHO ARE IN POSSESSION OF THE KEY AND UNINTELLIGIBLE TO ALL OTHERS THE USEFULNESS OF SUCH MESSAGES ESPECIALLY IN TIME OF WAR IS OBVIOUS H ON THE OTHER HAND THEIR SOLUTION MAY BE A MATTER OF GREAT IMPORTANCE TO THOSE FROM WHOM THE KEY IS CONC.

Q.11 Carmichael function:

$\lambda(n) = a^m \equiv 1 \bmod n$

for every a comprime to n

$m \rightarrow$ smallest positive integer

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

Given

$a^{n-1} \equiv 1 \bmod n$ Carmichael Number

n is odd composite

either $\lambda(n) = n-1$ or $\lambda(n) = n-1$

in both the case

$\frac{n-1}{\lambda(n)}$ · Remainder is zero

$K \in Z$

So $\frac{\lambda(n)}{n-1}$

Now second part

$\frac{\lambda(n)}{n-1}$ then n is Carmichael Number

$n-1 = K\lambda(n)$ — (1) integer

We know $\lambda(n)$ is smallest positive which satisfies $a^{\lambda(n)} \equiv 1 \bmod n$ — (II)

So any number of the form $K\lambda(n)$ also satisfy above equation (II)

$$a^{K\lambda(n)} \equiv 1 \bmod n$$

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

Hence proved Carmichael number

Q.15.
Ans.

SFA A: 45 ✓
Q = 30
Z = 26 ✓
L = 26 ✓
G = 25
S = 23 ✓
J = 21
M = 21

2 times 2 times
SFA - 5 times SF FA

(A → e) (1) e's frequency in the english alphabet

we can guess
S → T
F → H
Because THE Trigraph.

(e) AZ(+ 5 times , AZ 4 times
ZNA 2 times

- - (e)

ZLR 4 times
↓↓↓
and

No. 23
Date : / /

solar

① Z → A ② S → T
③ L → N ④ F → Y
⑤ R → D ⑥ A → E,

AQ - 2 times.
Q can be S.

⑪ Q → S

AZRRADQALSGZJ
eandessential

⑦ L → N
⑧ G → I
⑨ Z → A
⑩ J → L

BMJJADAJGCAGQZPA
dle eLi_eisa·e
f

⑫ C → f

⑬ k - m

SGKAGLZNAPQMLJGCAZ
timeina_e_S_n lifea
p r o

⑦ N → p ⑭ p - R ⑮ m - o

A U A P X m L A
E V E R 4 O N E

(16) 4 → V (17) X → 4

B M J J A D A
c o l l e g e

(18) B → C

A B C D E F G H I J K L M
Z E B R A C D F G H I J K

N O P Q R S T U V W X 4 Z
L M N O P Q S T U V W X 4.

Deciphered text:

College life is a remarkable and essential time in a person life and everyone should enjoy it college life teaches us many things and builds our confidence to face the new challenges and struggles in our future instead of just focusing on the study a person must participate in other activities and social is e as much as possible as all settings help in the overall development of a person.