Total No. of Printed Pages: 02

SUBJECT CODE NO: - Y-2050
FACULTY OF SCIENCE AND TECHNOLOGY
B.Sc. S.Y (Sem-III)
Examination March / April - 2023
Mathematics MAT - 301 Number Theory

[Time: 1:30 Hours] **[Max. Marks: 50]**

Please check whether you have got the right question paper.

N. B
i) All questions are compulsory.
ii) Figures to the right indicate full marks.

Q1 (a) Attempt any **one** of the following: 08

i. Given two integers a and b, with b > 0, then prove that there exist unique integers q and r such that

$$a = qb + r, 0 \leq r \leq b.$$

ii. If $k > 0$, then prove that $gcd\ (ka, kb) = k\ gcd\ (a, b)$.

(b) Attempt any **one** of the following: 07

i. By using the Euclidean algorithm, find the values of integers x and y satisfying $gcd(119, 272) = 119x + 272y$.

ii. If a and b are both odd integers, the prove that 16| $a^4+b^4- 2$.

Q2 a) Attempt any **one** of the following: 08

i. If n> 1 is a fixed integer and a, b, c, d are arbitrary integers, then prove that

$\alpha)\ If\ a \equiv b(mod n)\ and\ c \equiv d(mod n), then\ a + c \equiv b + d(mod n).$

$\beta)\ If\ a \equiv b(mod n)\ and\ c \equiv d(mod n), then\ ac \equiv bd(mod n).$

ii. State and prove Fermat's theorem

b) Attempt any **one** of the following: 07

i. Solve the following set of simultaneous congruences

$$x \equiv 2(mod 3), x \equiv 3(mod 5), x \equiv 2(mod 7).$$

ii. Find the remainder when 15! is divided by 17.

3CFA2980EA5E5EF2EE5F23CA480B4B31

Q3 (a) Attempt any **one** of the following: 05

i. Prove that the functions σ *and* τ are multiplicative functions.

ii. If $n \geq 1$ *and* $gcd(a, n) = 1$, then prove that $a^{\phi(n)} = 1(mod n)$.

(b) Attempt any **one** of the following: 05

i. Find $\phi(36000)$.

ii. Prove that any prime of the form $3n + 1$ is also of the form $6m + 1$.

Q4 Choose the correct alternative and **rewrite the sentence:** 10

a) Two integers a and b not both of which are zero are said to be relatively prime, if ----------

i) $gcd\,(a, b) = 0$
ii) $gcd(a, b) = 1$
iii) $gcd(a, b) = a$
iv) $gcd(a, b) = b$

b) If $d = gcd(a, n)$, then the linear congreunce $ax \equiv b(mod n)$ has a solution if and only if ....

i) $d|a$
ii) $d|b$
iii) $b|d$
iv) $a|d$

c) The value of $(30) =$ ......

i) 1
ii) 0
iii) 3
iv) -1

d) If n is even integer, then $\phi(2n) =$

i) $2\phi(n)$
ii) $2n$
iii) n
iv) $\phi(n)$

e) A composite integer n is called a pseudoprime, if ....

i) $n|2^n + 2$
ii) $n\,|2^n - 2$
iii) $n|2^n - 1$
iv) $n\,|2^n$

3CFA2980EA5E5EF2EE5F23CA480B4B31