

U.G. 5th Semester Examination - 2024**MATHEMATICS****[HONOURS]****Discipline Specific Elective (DSE)****Course Code : MATH-H-DSE-T-2A****(Number Theory)****[New Syllabus]****Full Marks : 60****Time : $2\frac{1}{2}$ Hours***The figures in the right-hand margin indicate marks.**Symbols and notations have their usual meanings.*

1. Answer any ten questions: $2 \times 10 = 20$
- a) If a prime p divides ab , then prove that $p|a$, or $p|b$.
 - b) Let $\gcd(a, b) = 1$. Prove that $\gcd(a + b, a - b)$ is either 1 or 2.
 - c) Prove that if $2^n + 1$ is prime, then n is a power of 2.
 - d) Let μ denotes the Möbius function $n \in \mathbb{N}$ and $n > 1$. Then show that

$$\sum_{d|n} \mu(d) = \left(\frac{1}{n}\right)$$

[Turn over]

e) Show that $\tau(n)$ is odd if and only if n is a square, where $\tau(n)$ denotes the number of positive divisors of n .

f) Let $\phi(n)$ denotes the Euler totient function. if $m|n$, then prove that $\phi(m)|\phi(n)$.

g) State Wolstenholme's theorem.

h) Solve the congruence $4x \equiv 26 \pmod{33}$.

i) Let p be a natural number such that $(p-1)! \equiv -1 \pmod{p}$. Prove that p is a prime number.

j) Find all n for which $\phi(n) \equiv 2 \pmod{4}$.

k) Define Legendre's symbol $(n|p)$.

l) Calculate $(2|5)$.

m) Prove that m is prime if and only if $\exp_m(a) = m-1$ for some a .

n) Determine whether 219 is a quadratic residue or non-residue mod 383.

o) Discuss RSA encryption and decryption.

2. Answer any four questions: 5×4=20

a) State and prove the Euclidean algorithm.

b) The sum of two positive integers is 5264 and their least common multiple is 200340. Determine the two integers.

c) Let $\phi(n)$ denotes the Euler totient function. If $n \geq 1$, then prove that

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

d) State and prove the Fermat's little theorem.

e) State and prove the principle of cross-classification.

f) Prove that $5n^3 + 7n^5 \equiv 0 \pmod{12}$ for all integers n .

3. Answer any two questions: 10×2=20

a) i) State and prove the Lagrange's theorem for polynomial congruence.

ii) Solve the following system of congruences:

$$x \equiv 1 \pmod{4}, \quad x \equiv 2 \pmod{5}, \quad x \equiv 3 \pmod{7}.$$

5+5

b) i) State and prove the Eulers criterion related to the Legendre's symbol.

ii) Evaluate $(5|3)(3|5)$. 5+5

c) Prove that

i) $1^{2^3} 3^{2^5} 5^{2^2} \dots 11^{2^2} \equiv -1 \pmod{13}.$

ii) $2^{2^4} 4^{2^6} 6^{2^2} \dots 12^{2^2} \equiv -1 \pmod{13}.$ 5+5

d) i) State and prove the Möbius inversion formula.

ii) Solve $8^x \equiv 3 \pmod{43}.$ 5+5
