DHANAMANJURI UNIVERSITY

Examination- 2025 (June)

Four-year course B.A/B.Sc. 6^{th} Semester (NEP)

Name of Programme	**:**	**B.A. / B.Sc. Mathematics (Honours)**
Paper Type	**:**	**DSE**
Paper Code	**:**	**EMA-002**
Paper Title	**:**	**Number Theory**
Full Marks	**:**	**80**
Pass Marks	**:**	**32**

Duration: 3 Hours

The figures in the margin indicate full marks for the questions.
Answer all the questions:

1. Choose and rewrite the correct answer for each of the following: **1×3=3**

a) The exponent of the highest power of 2 that divides 50! is

i) 45

ii) 47

iii) 50

iv) 52

b) Consider the following statements:

S_1 : 15 has a primitive root

s_2 : 18 has a primitive root.

Then

i) both S_1 and S_2 are true.

ii) neither S_1 nor S_2 is true.

iii) only S_1 is true.

iv) only S_2 is true.

c) What is the value of the Legendre symbol $(-1/p)$ if $p \equiv 1 \ (mod\ 4$?

i) -1

ii) 0

iii) 1

iv) 4

2. Write very short answer for each of the following questions: **1×6=6**

a) Evaluate $\tau(2200)$, where $\tau(n)$ denote the number of positive divisors of n.

b) Find the order of the integer 5 modulo 13.

c) Write the number of primitive roots of 17.

d) State Euler's criterion.

e) Write the quadratic residues of 11.

f) Let a be an odd integer such that $x^2 \equiv a \ (mod\ 32)$ has a solution. What can you say about the values of a?

3. Answer the following questions: **3×5=15**

a) Show that $\sqrt{2}$ is irrational.

b) If F is a multiplicative function and $F(n) = \sum_{d|n} f(d)$, then show that f is also multiplicative.

c) If the integer a has order k modulo n and $h > 0$, then prove that a^h has order $k/gcd\ (h, k)$ modulo n.

d) Show that the only incongruent solutions of $x^2 \equiv 1 \ (mod\ p)$ are 1 and $p - 1$, where p is an odd prime.

e) Find the value of the Legendre symbol $(219/383)$.

4. Answer the following questions: **4×5=20**

a) Solve the linear Diophantine equation $172x + 20y = 1000$.

b) Show that $53^{103} + 103^{53}$ is divisible by 39.

c) Prove that the integer $2^k, k \geq 3$ has no primitive roots.

d) Let p be an odd prime. Prove that

$$(2/p) = \begin{cases} 1, & if\ \boldsymbol{p} \equiv 1 \ (mod\ 8)\ or\ \boldsymbol{p} \equiv 7 \ (mod\ 8) \\ -1, & if\ \boldsymbol{p} \equiv 3 \ (mod\ 8)\ or\ \boldsymbol{p} \equiv 5 \ (mod\ 8) \end{cases}.$$

e) If p is an odd prime, then prove that $\sum_{a=1}^{p-1}(a/p) = 0$.

5. **Answer any two of the following questions:** **6×2=12**

a) State and prove Fundamental Theorem of Arithmetic.

b) Solve the system of congruences

$x \equiv 3\ (mod\ 5), \quad x \equiv 2\ (mod\ 7), \quad x \equiv 6\ (mod\ 11).$

c) State and prove Wilson's theorem.

6. **Answer any two of the following questions:** **6×2=12**

a) If p is a prime and

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \not\equiv 0\ (mod\ p)$

is a polynomial of degree $n \geq 1$ with integral coefficients, then prove that the congruence $f(x) \equiv 0\ (mod\ p)$ has at most n incongruent solutions modulo p.

b) Let p be a prime number and $d|p-1$. Prove that there are exactly $\phi(d)$ incongruent integers having order d modulo p.

c) Solve the quadratic congruence
$3x^2 + 9x + 7 \equiv 0(mod\ 13)$.

7. **Answer any two of the following questions:** **6×2=12**

a) State and prove Gauss's lemma.

b) If p is an odd prime and $gcd\ (a, p) = 1$, then prove that the congruence

$$x^2 \equiv a\ (mod\ p^n), n \geq 1$$

has a solution if and only if $(a/p) = 1$.

c) Given the RSA algorithm parameters where $p = 2, q = 11$ and $k = 3$, calculate the public key (n, k) and the private key j. Also, encrypt the message $M = 5$ using the public key and then decrypt it using the private key to verify the correctness of the encryption and decryption process.

*****