DHANAMANJURI UNIVERSITY

Examination- 2026 (June)

Name of Programme : **B.A./ B.Sc. Mathematics**
Semester : **6th**
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. **Write very short answer for each of the following questions:** $1 \times 5 = 5$

   a) Write the condition for the system of linear congruences
   $$ax + by \equiv r \ (mod\ n)$$
   $$cx + dy \equiv s \ (mod\ n)$$
   to have a unique solution modulo n .

   b) Find the order of 2 modulo 11.

   c) Write the highest power of 5 dividing 100!.

   d) Define quadratic residue of an odd prime.

   e) State Quadratic Reciprocity law.

2. **Write short answer the following questions:** $3 \times 5 = 15$

   a) Find the units digit of 3^{100}.

   b) If p and q are distinct primes, then show that $p^{q-1} + q^{p-1} \equiv 1 \ (mod\ pq)$.

   c) Find all the primitive roots of 26.

   d) If the integer a has order k modulo n, then prove that $a^i \equiv a^j \ (mod\ n)$ iff $i \equiv j \ (mod\ k)$.

e) Determine whether the quadratic congruence $x^2 \equiv 219 \pmod{419}$ is solvable.

3. **Answer the following questions:** $4 \times 6 = 24$

a) Show that Mobius function μ is multiplicative.

b) i) If $a|c$ and $b|c$ with $(a, b) = 1$, then prove that $ab|c$.

ii) Show that $a|c$ if $a|bc$ with $(a, b) = 1$.

c) Let the integer a has order k modulo n. Then prove that $a^h \equiv 1 \pmod{n}$ iff $k|h$.

d) Prove that if n has a primitive root, then it has exactly $\phi(\phi(n))$ of them.

e) If p is an odd prime, then prove that there are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non residues of p.

f) Prove that if p is any odd prime, and a relatively prime to p, then show that the Legendre symbol satisfies

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \quad \text{and} \quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

4. **Answer any two of the following questions:** $6 \times 2 = 12$

a) Show that the linear congruence $a \equiv b \pmod{n}$ has a solution iff d|b where d=(a, n). Also prove that if d|b, it has d mutually incongruent solutions modulo n.

b) Prove that the Fermat number F_n is prime iff $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

c) State and prove Euler's theorem.

5. **Answer any two of the following questions:** $6 \times 2 = 12$

a) Let p be a prime number and $d|p-1$, then prove that the congruence $x^d - 1 \equiv 0 \pmod{p}$ has exactly d solutions.

b) State and prove Euler's criterion.

c) Prove that for any odd prime p and $k \geq 1$, there exists a primitive root for p^k.

6. Answer any two of the following questions: $6 \times 2 = 12$

a) Let p be an odd prime and a an odd integer with $(a, p)=1$, then show that $\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]}$.

b) Let a be an odd integer, then prove that

i) $x^2 \equiv a \ (mod\ 2)$ always has a solution.

ii) $x^2 \equiv a \ (mod\ 4)$ has a solution iff $a \equiv 1 \ (mod\ 4)$.

iii) $x^2 \equiv a \ (mod\ 2^n)$ for $n \geq 3$ has a solution iff $a \equiv 1 \ (mod\ 8)$

c) Using the RSA algorithm, generate a public key and private key where $p = 5, q = 13$. Also, encrypt the message $M = G$ using the public key and then decrypt it using the private key.

*****