LOYOLA COLLEGE (AUTONOMOUS) CHENNAI – 600 034

M.Sc. DEGREE EXAMINATION – **MATHEMATICS**

THIRD SEMESTER – **APRIL 2025**

PMT3MC02 – NUMBER THEORY

Date: 26-04-2025 Dept. No. Max. : 100 Marks

Time: 09:00 AM - 12:00 PM

	SECTION A – K1 (CO1)
	Answer ALL the questions **(5 x 1 = 5)**
1	**Answer the following**
a)	Does the following statement: "If m and n are positive integers, $m \mid n$ and $n \mid m$ then $m = n$" holds? Justify.
b)	State Chinese remainder theorem.
c)	What are the two basic problems that dominate the theory of quadratic residues?
d)	Define primitive root.
e)	Write any two advantages of public key cryptography.
	SECTION A – K2 (CO1)
	Answer ALL the questions **(5 x 1 = 5)**
2	**MCQ**
a)	The linear combination of $(252,198) = 18$ is (i) $252 \times 4 - 198 \times 5$ (ii) $252 \times 5 - 198 \times 4$ (iii) $252 \times 5 - 198 \times 2$ (iv) $252 \times 4 - 198 \times 4$
b)	If a is a whole number and p is a prime number then (i) $a^{p-1} - a$ is divisible by p (ii) $a^p - 1$ is divisible by p (iii) $a^p - a$ is not divisible by p (iv) $a^p - a$ is divisible by p
c)	If P is an odd positive integer then $\left(-1 \mid P\right)$ is (i) $(-1)^{\frac{P-1}{2}}$ (ii) $(-1)^{\frac{P^2-1}{2}}$ (iii) $(-1)^{\frac{P^2-1}{8}}$ (iv) $(-1)^{\frac{P-1}{8}}$
d)	The exponent of 3 modulo 8 is (i) 4 (ii) 2 (iii) 8 (iv) 16
e)	The inverse of 17 modulo 29 is (i) 6 (ii) 9 (iii) 15 (iv) 12
	SECTION B – K3 (CO2)
	Answer any THREE of the following **(3 x 10 = 30)**
3	State and prove the properties of greatest common divisor.
4	For a given modulus m, show that (i) $\hat{a} = \hat{b}$ if and only if $a \equiv b(mod\ m)$ (ii) Two integers x and y are in the same residue class if and only if $x \equiv y(mod\ m)$ (iii) The m residue classes $\hat{1}, \hat{2}, \ldots, \hat{m}$ are disjoint and their union is the set of all integers.
5	Show that the Legendre's symbol $\left(n \mid p\right)$ is completely multiplicative function of n.
6	Find the primitive roots of 17.
7	In a long string of ciphertext which was encrypted by means of an affine map on single letter message units in the 26-letter alphabet. You observe that the most frequently occurring letters are "K" and "D" in that order. Assuming that those ciphertext message units are the encryption of "E" and "T" respectively. Develop the deciphering formula with appropriate keys.

	SECTION C – K4 (CO3)
	Answer any TWO of the following **(2 x 12.5 = 25)**
8	State and prove Euler's summation formula.
9	Solve $x \equiv 4(mod\ 11); x \equiv 5(mod\ 7)$ and $x \equiv 6(mod\ 13)$.
10	Determine whether 219 is a quadratic residue or nonresidue mod 383.
11	Given $m \geq 1$, $(a, m) = 1$ and let $f = exp_m(a)$. Then show that (i) $a^k \equiv a^h(mod\ m)$ if and only if $k \equiv h(mod\ m)$ (ii) $a^k \equiv 1(mod\ m)$ if and only if $k \equiv 0(mod\ m)$. In particular, $f \mid \varphi(m)$ (iii) The numbers $1, a, a^2, \ldots, a^{f-1}$ are incongruent modulo m.
	SECTION D – K5 (CO4)
	Answer any ONE of the following **(1 x 15 = 15)**
12	Explain Euler's totient and analyze Euler-Fermat theorem with an appropriate proof.
13	Analyze Gauss lemma with a suitable proof.
	SECTION E – K6 (CO5)
	Answer any ONE of the following **(1 x 20 = 20)**
14	(i) Given integers a and b with $b > 0$, prove that there exists a unique pair of integers q and r such that $a = bq + r$ with $0 \leq r < b$. Moreover, show that $r = 0$ if and only if $b \mid a$. (12 marks) (ii) If the exponent of a and b modulo m are f and g respectively and $(f, g) = 1$, then prove that the exponent of ab modulo m is fg. (8 marks)
15	(i) Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(Z/NZ)$ and set $D = ad - bc$, then justify that the following statements are equivalent (a) g.c.d $(D, N) = 1$ (b) A has an inverse matrix (c) if x and y are not both 0 in Z/NZ then $A\begin{pmatrix} x \\ y \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ (d) A gives a 1-1 correspondence of $(Z/NZ)^2$ with itself. (10 marks) (ii) Encipher the message "PAYMENOW" using affine transformation with enciphering key $a = 7$ and $b = 12$. (10 marks)

$$$$$$$$$$$$$