LOYOLA COLLEGE (AUTONOMOUS) CHENNAI – 600 034

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

THIRD SEMESTER – **NOVEMBER 2024**

PMT3MC02 – NUMBER THEORY

Date: 09-11-2024 Dept. No. Max. : 100 Marks

Time: 01:00 pm-04:00 pm

	SECTION A – K1 (CO1)
	Answer ALL the questions **(5 x 1 = 5)**
1	**Answer the following**
a)	Does the following statement: “If a prime p does not divide a then $(p,a)=1$” holds? Justify.
b)	State Little Fermat theorem.
c)	What are the two basic problems that dominate the theory of quadratic residues?
d)	Check 2 is a primitive root of 11.
e)	Define encryption.
	SECTION A – K2 (CO1)
	Answer ALL the questions **(5 x 1 = 5)**
2	**MCQ**
a)	If the GCD of 65 and 117 is expressible in the form $65m-117$ then the value of m is ___________ (i) 4 (ii) 2 (iii) 1 (iv) 3
b)	The solution of the linear congruence $4x\equiv 5(mod\,9)$ is (i) 6 (mod 9) (ii) 8 (mod 9) (iii) 9 (mod 9) (iv) 11 (mod 9)
c)	The Diophantine equation $y^2=x^3+k$ has ________ number of solutions when $k=(4n-1)^3-4m^3$. (i) 0 (ii) 1 (iii) 2 (iv) 3
d)	If the exponent of a modulo m is f, then the exponent of a^k modulo m is _______. (i) $f\times(f,k)$ (ii) $f+(f,k)$ (iii) $\frac{f}{(f,k)}$ (iv) $\frac{(f,k)}{f}$
e)	Suppose in the 26-letter alphabet, the digraph enciphering transformation $C=159P+580$ modulo 676. The digraph “ON” is encrypted as _______. (i) QY (ii) NV (iii) ZA (iv) IW
	SECTION B – K3 (CO2)
	Answer any THREE of the following **(3 x 10 = 30)**
3	State and prove Euclidean algorithm.

4	Assume $(a,m)=d$ and suppose that $d \mid p$. Then show that the linear congruence $ax \equiv b \pmod m$ has exactly d solutions modulo m. These are given by $t, t+\frac{m}{d}, \ldots, t+(d-1)\frac{m}{d}$, where t is the solution modulo $\frac{m}{d}$, of the linear congruence $\frac{a}{d}x \equiv \frac{b}{d}\left(mod\ \frac{m}{d}\right)$.
5	State and prove Euler's criterion.
6	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.
7	Encipher the message "PAYMENOW" using affine transformation with enciphering key $a=7$ and $b=12$.
	SECTION C – K4 (CO3)
	Answer any TWO of the following **(2 x 12.5 = 25)**
8	State and prove the properties of divisibility.
9	Solve $x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 5$ and $x \equiv 2 \pmod 7$.
10	Determine whether 219 is a quadratic residue or nonresidue mod 383.
11	Examine that in every reduced residue system mod p there are exactly $\varphi(d)$ numbers $'a'$ such that $\exp_p(a)=d$ for an odd prime p and d, any positive divisor of $p-1$.
	SECTION D – K5 (CO4)
	Answer any ONE of the following **(1 x 15 = 15)**
12	Explain Jacobi symbol and prove all its properties.
13	If $a \equiv b \pmod m$ and $\alpha \equiv \beta \pmod m$ then prove that (i) $ax+\alpha y \equiv bx+\beta y \pmod m$ for all integers x and y. (ii) $a\alpha \equiv b\beta \pmod m$ (iii) $a^n \equiv b^n \pmod m$ for every positive integer n. (iv) $f(a) \equiv f(b) \pmod m$ for every polynomial f with integer coefficients.
	SECTION E – K6 (CO5)
	Answer any ONE of the following **(1 x 20 = 20)**
14	(i) State Fundamental theorem of arithmetic and examine it with an appropriate proof. (12 marks) (ii) If $n \geq 1$, then show that $\sum_{d \mid n} \varphi(d) = n$. (8 marks)
15	Suppose that we know that our adversary is using a 2×2 enciphering matrix with a 29-letter alphabet, where $A-Z$ have the numerical equivalents 0 – 25, blank = 26, ? = 27, ! = 28. We receive the message "GFPYJP X?UYXSTLADPLW" and suppose that we know that the last five letters of

	plaintext are our adversary signature “KARLA”. Decipher the above message.

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