LOYOLA COLLEGE (AUTONOMOUS), CHENNAI – 600 034

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

THIRD SEMESTER – **NOVEMBER 2023**

PMT3MC02 – NUMBER THEORY

Date: 01-11-2023 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: "For all integers a and b, if $a \mid b$ and $b \mid a$ then $a = b$" holds? Justify.
b)	Define reduced residue system.
c)	State the reciprocity law for Jacobi symbol.
d)	Let g be a primitive root mod p, where p is an odd prime. Then what are the quadratic residues and non-residues mod p?
e)	Write any two applications for public key cryptography?
	SECTION A – K2 (CO1)
	Answer ALL the questions **(5 x 1 = 5)**
2.	**Choose the correct answer**
a)	The greatest common divisor of 4598 and 3211 is (i) 21 (ii) 19 (iii) 23 (iv) 17
b)	Let k be the order of $a\ mod\ n$ then $a^b \equiv 1(mod\ n)$ if and only if (i) k divides a (ii) k divides b (iii) k divides n (iv) k divides 1
c)	If P is an odd positive integer then $(2 \mid P)$ 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)	If a is a primitive root of modulo m, then (i) $exp_m(a) \le \varphi(m)$ (ii) $exp_m(a) = \varphi(m)$ (iii) $exp_m(a) \ge \varphi(m)$ (iv) $exp_m(a) < \varphi(m)$
e)	Suppose in the 26-letter alphabet, the transformation $f(P) \equiv P + 3\ mod\ 26$. The word "YES" is encrypted as (i) BHV

	(ii) ZKB (iii) FQO (iv) DEM
SECTION B – K3 (CO2)	
	Answer any THREE of the following **(3 x 10 = 30)**
3.	State and prove Fundamental theorem of arithmetic.
4.	Solve $9x \equiv 21(mod\ 30)$.
5.	Examine that the Diophantine equation $y^2 = x^3 + k$ has no solution if k has the form $k = (4n-1)^3 - 4m^2$, where m and n are integers such that no prime $p \equiv -1(mod 4)$ divides m.
6.	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 $k \equiv 0(mod\ m)$. I particular, $f \mid \varphi(m)$ (iii) The numbers $1, a, a^2, \dots, a^{f-1}$ are incongruent modulo m.
7.	Working in the 26-letter alphabet, use the matrix $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$, to encipher the message unit “NO” and decipher the ciphertext “FWMDIQ”.
SECTION C – K4 (CO3)	
	Answer any TWO of the following **(2 x 12.5 = 25)**
8.	State and prove Euler’s summation formula.
9.	Assume $(a,m) = d$ and suppose that $d \mid p$. Then show that the linear congruence $ax \equiv b(mod\ m)$ has exactly d solutions modulo m. These are given by $t, t + \frac{m}{d}, \dots, t + (d-1)\frac{m}{d}$, where t is the solution modulo $\frac{m}{d}$, of the linear congruence $\frac{a}{d}x \equiv \frac{b}{d}\left(mod\ \frac{m}{d}\right)$.
10.	Explain Legendre’s symbol $(n \mid p)$ and show that it is completely multiplicative function of n.
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.	(a) Determine the exponent of (i) 3 modulo 7 and (ii) 2 modulo 11. (8 marks) (b) State and prove Euclid’s theorem. (7 marks)
13.	Justify the Chinese remainder theorem with a suitable proof and hence evaluate $x \equiv 2(mod\ 3); x \equiv 3(mod\ 5)$ and $x \equiv 2(mod\ 7)$.
SECTION E – K6 (CO5)	
	Answer any ONE of the following **(1 x 20 = 20)**
14.	(a) Explain Jacobi symbol and prove all its properties. (15 marks) (b) 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. (5 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.

###########