Sanjay Ghodawat University, Kolhapur
Established as State Private University under Govt. of Maharashtra.
Act No XL, 2017

2018-19
EXM/P/09/00

Year and Program: 2018-2019 M.Sc. | **School of Science** | **Department of Mathematics**

Course Code – MTS 608
Day and Date – Tuesday 28/05/2019
PRN number –

Course Title – Number Theory
End Semester Examination
Seat no- (A)

Semester – IV
Time: 2:30 to 3:00 pm
Max Marks: 100
Answer Booklet No.-

Students' Signature -

Invigilator's Signature –

Instructions:

1) All questions are compulsory.
2) **Attempt Q.1 within first 30 minutes.**
3) Each MCQ type question is followed by four plausible alternatives, Tick (√) the correct one.
4) Answer to question 1 should be written in the question paper and submit to the Jr. Supervisor.
5) If you tick more than one option it will not be evaluated
6) Figures to the right indicate full marks
7) Use **Blue ball pen** only.
8) $\tau(n)$ stands for number of positive divisors of n
9) $\sigma(n)$ stands for sum of positive divisors of n
10) φ stands for Euler's totient function

Q.1	Tick Mark correct alternative	Marks	Bloom's Level	CO
i)	Which of the following linear Diophantine equation is not solvable? a) $6x + 51y = 22$ c) $x + 4y = 44$ b) $172x - 20y = 1000$ d) $3x + 6y = 18$	2	L4	CO1
ii)	One of the solutions for the equation $18x \equiv 30\ (mod\ 42)$ is a) 10 b) 11 c) 12 d) 13	2	L4	CO2
iii)	What is the unit place value of 2^{100}? a) 2 b) 4 c) 6 d) 8	2	L5	CO3

ESE
page 1/2

iv)	The number of elements in the set $\{m\ :1 \leq m \leq 500,\ m \text{ and } 500 \text{ are relatively prime}\}$ is a) 100 b) 200 c) 300 d) 400	2	L5	CO4
v)	If n is a positive integer and a is any integer relatively prime to n then a) $a^{\varphi(n)} \equiv 1\ (mod\ n)$ c) $a^{\varphi(n)} \equiv 0\ (mod\ n)$ b) $a^{\varphi(n)} \equiv 2\ (mod\ n)$ d) $a^{\varphi(n)} \equiv (n+1)\ (mod\ n)$	2	L2	CO4
vi)	If $\gcd(a,\ k) = 1$ then $a^{24} - 1$ is divisible by k, then k is a) 5 b) 10 c) 15 d) 20	2	L5	CO4
vii)	For any prime $p,\ \varphi(p)$ is ______ a) Even integer c) Odd integer b) Prime number d) None of these	2	L4	CO4
viii)	Let the integer a have order k modulo n. Consider the statements **A:** $a^b \equiv 1(mod\ n)$ iff $k\|\varphi(n)$ **B:** $a^i \equiv a^j(mod\ n)$ iff $i \equiv j(mod\ k)$ a) A is true but B is false c) B is true but A is false b) Both A and B are true d) Both A and B are false	2	L5	CO5
ix)	Which of the following is quadratic residue of 13? a) 2 b) 3 c) 5 d) 8	2	L2	CO5
x)	Order of 2 modulo 13 is ______ a) 2 b) 4 c) 6 d) 12	2	L5	CO5

*****

ESE

page 2/2

Year and Program: 2018-2019 M.Sc.	**School of Science**	**Department of Mathematics**
Course Code: MTS 608	**Course Title: Number Theory**	**Semester – IV**
Day and Date: Tuesday 28/05/2019	**End Semester Examination (ESE)**	**Time:** 3.00 to 5.30 pm
		Max Marks: 100

Instructions:

1) All questions are compulsory.
2) Figures to the right indicate full marks.
3) Non-programmable calculator is allowed

			Marks	Bloom's Level	CO
Q.2		**Solve any TWO**			
	i)	If a and b are positive integers then create the relation between $gcd(a,b)$ and $lcm(a,b)$	6	L6	CO1
	ii)	Show that if a and b are given integers not both zero then the set $T = \{ax + by \| x, y \in Z\}$ is precisely the set of all multiples of d, Where $d = g.c.d(a,\ b)$	6	L2	CO1
	iii)	Show that there are infinite number of primes of the form $(4n + 3)$	6	L4	CO1
Q.3		**Solve any TWO**			
	i)	Let $n > 0$ be fixed and a, b, c be arbitrary integers. Show that a) If $a \equiv b(mod\ n)$ and $c \equiv d(mod\ n)$ then $ac \equiv bd(mod\ n)$ b) If $a \equiv b(mod\ n)$ then $a^k \equiv b^k(mod\ n)$ for any $k \in Z$	7	L3	CO2
	ii)	Show that the linear congruence $ax \equiv b(mod\ n)$ has a solution iff $d\|b$; where $d = g.c.d(a,n)$, also if $d\|b$ then show that it has d mutually incongruent solution modulo n.	7	L2	CO2
	iii)	State and prove Chinese Remainder Theorem.	7	L1	CO2
Q.4		**Solve any TWO**			
	i)	If p and q are distinct primes such that $a^p \equiv a(mod\ q)$ and $a^q \equiv a(mod\ p)$ then show that $a^{pq} \equiv a(mod\ pq)$ and hence prove that $2^{341} \equiv 2(mod\ 341)$	7	L3	CO3
	ii)	If $n = {p_1}^{k_1}.{p_2}^{k_2}.{p_3}^{k_3}.\cdots {p_r}^{k_r}$ is the prime factorization of $n > 1$ then show that $\tau(n) = (k_1 + 1)(k_2 + 1)(k_3 + 1)\cdots(k_r + 1)$ $\sigma(n) = \frac{{p_1}^{k_1+1} - 1}{(p_1 - 1)}.\frac{{p_2}^{k_2+1} - 1}{(p_2 - 1)}.\frac{{p_3}^{k_3+1} - 1}{(p_3 - 1)}.\cdots\frac{{p_r}^{k_r+1} - 1}{(p_r - 1)}$	7	L4	CO3
	iii)	Define a) Pseudoprime b) Absolute pseudoprime and prove that 561 is absolute pseudoprime.	7	L3	CO3

Q.5	**Solve any FOUR**			
i)	Show that $gcd(a, bc) = 1$ iff $gcd(a, b) = 1$ and $gcd(a,\ c) = 1$	5	L4	CO4
ii)	If the integer $n > 1$ has a prime factorization $n = {p_1}^{k_1}.{p_2}^{k_2}.{p_3}^{k_3}.\cdots {p_r}^{k_r}$ then show that $\varphi(n) = ({p_1}^{k_1} - {p_1}^{k_1-1})({p_2}^{k_2} - {p_2}^{k_2-1})\cdots({p_r}^{k_r} - {p_r}^{k_r-1})$	5	L2	CO4
iii)	Show that $\varphi(n)$ is an even integer for any $n > 2$.	5	L4	CO4
iv)	Show that $n = \sum_{d\mid n} \varphi(d)$, where d runs all positive divisor of n.	5	L2	CO4
v)	Find a) $\varphi(50000)$; b) $\varphi(360)$	5	L3	CO4
vi)	If n is a positive integer and $gcd\ (a,\ n) = 1$ then show that $a^{\varphi(n)} \equiv 1(mod\ n)$	5	L2	CO4
Q.6	**Solve any FOUR**			
i)	Let $gcd(a, n) = 1$ and the integer a have order k modulo n and $a^b \equiv 1(mod\ n)$ analyze the relation between b and k	5	L4	CO5
ii)	If the integer a has order k modulo n and $b > 0$ then show that a^b has order $\frac{k}{g.c.d(b,\ k)}$ $modulo\ n.$	5	L2	CO5
iii)	If p is an odd prime and $gcd\ (a,\ p) = 1$, then show that a is a quadratic residue of p iff $a^{\left(\frac{p-1}{2}\right)} \equiv 1\ (mod\ p)$.	5	L2	CO5
iv)	Let p be an odd prime and a, b be integers which are relatively prime to p. Show that a) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ b) $\left(\frac{1}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)}$	5	L1	CO5
v)	Show that the congruence $x^2 \equiv -38\ (mod\ 13)$ has a solution.	5	L3	CO5
vi)	If p is an odd prime, then show that $\left(\frac{2}{p}\right) = (-1)^{\left(\frac{p^2-1}{8}\right)}$.	5	L1	CO5

****

ESE