SEAT No.________

[72/AU6]

No of printed pages : 3

SARDAR PATEL UNIVERSITY
B.Sc.(SEMESTER - V) EXAMINATION (NC)
Friday, 13-04-2018
MATHEMATICS : US05CMTH05
(Number Theory)

Time : 02:00 p.m. to 05:00 p.m. Maximum Marks : 70

Que.1 Fill in the blanks. 10

(1) If n is odd integer then $3^n + 1$ is divisible by ....

(a) 5 (b) 3 (c) 4 (d) 6

(2) $(a\ ,\ b) \geq$ .... $\forall\ a\ ,\ b \in \mathbb{Z}$.

(a) a (b) b (c) 0 (d) 1

(3) $(a\ ,\ c) = (b\ ,\ c) = 1$ then ....

(a) $(ab\ ,\ c) = 1$ (b) $(a\ ,\ b) = 1$ (c) $(a\ ,\ b)c = 1$ (d) $a = b = 1$

(4) .... is Fermat's number .

(a) 100 (b) 116 (c) 327 (d) 257

(5) $F_0F_1F_2$...........F_{n-1} = ...

(a) $F_n + 2$ (b) F_{n+2} (c) $F_n - 2$ (d) F_{n-2}

(6) $\mu(12)$ = ...

(a) 1 (b) 0 (c) -1 (d) 3

(7) 765432 is not divisible by ....

(a) 7 (b) 3 (c) 4 (d) 9

(8) $\phi(m) + S(m) = mT(m)$ iff m is ....

(a) not prime (b) odd (c) even (d) prime

(9) $18x \equiv 30(mod\ 42)$ has only .... solutions.

(a) 3 (b) 2 (c) 1 (d) 6

(10) ϕ (128) = ...

(a) 128 (b) 16 (c) 64 (d) 32

(P.T.O.)

Que.2 Answer the following (Any Ten) 20

(1) Prove that $(a+b)[a,b] = b[a, a+b]$, $\forall\ a\ ,\ b > 0$.

(2) State and prove Euclid's result for prime number.

(3) Find $(136, 228, 392)$.

(4) Find highest power of 3 in 50! .

(5) Prove that $[x] + [y] \leq [x+y] \leq [x] + [y] + 1$.

(6) If a and b are relatively prime numbers then prove that P(ab) $= P(a)^{T(b)} P(b)^{T(a)}$.

(7) If $a \equiv b (mod\ n)$,then prove that $a^m \equiv b^m (mod\ n)$, $\forall\ m \in \mathbb{N}$, by using mathematical induction method.

(8) Find positive integer solution of $7x + 19y = 213$.

(9) Find all relatively prime solution of $x^2 + y^2 = z^2$ with $0 < z < 30$.

(10) Find $\phi(243) + \phi(81) + \phi(27) + \phi(9) + \phi(3)$.

(11) Solve the equation $103x \equiv 57 (mod\ 211)$.

(12) Find order of 5 modulo 13 .

Que.3 (a) Prove that there are infinitely many prime number of the form $4n - 1$. 3

(b) Prove that $[a, b, c] = \dfrac{abc}{(ab, bc, ca)}$, $\forall\ a\ ,\ b\ ,\ c > 0$. 3

(c) State and prove Fundamental theorem of divisibility. 4

OR

Que.3 (a) Let g be a positive integer greater than 1 then prove that every positive integer a can can be written uniquely in the form $a = c_n g^n + c_{n-1} g^{n-1} + ... + c_1 g + c_0$, where $n \geq 0$, $c_i \in \mathbb{Z}$, $0 \leq c_i < g$, $c_n \neq 0$. 5

(b) State and prove fundamental theorem of arithmetic . 5

Que.4 (a) Prove that odd prime factor of M_p $(p > 2)$ has the form $2pt + 1$, for some integer t. 5

(b) Define Mersenne number.Prove that any prime factor of M_p is greater than p. 5

OR

Que.4 (a) Prove that every prime factor of F_n $(n > 2)$ is of the form $2^{n+2}t + 1$, for some integer t. 5

(b) Let x be any positive real number and n be any positive integer then prove that among the integers from 1 to x the number of multipliers of n is $\left[\dfrac{x}{n}\right]$. 3

(c) Prove that $(u_m, u_n) = u_{(m,n)}$. 2

Que.5 (a) Prove that $x^4 + y^4 = z^2$ has no nonzero positive integer solution . Hence prove that $x^{-4} + y^{-4} = z^{-4}$ has no nonzero positive integer solution . 7

(b) Find a necessary and sufficient condition that a positive integer is divisible by 13. 3

OR

Que.5 (a) Prove that the integer solution of $x^2 + 2y^2 = z^2$, $(x, y) = 1$ can be expressed as $x = \pm(a^2 - 2b^2)$, $y = 2ab$, $z = a^2 + 2b^2$. 6

(b) Find positive integer solution of $19x + 20y = 1909$ 4

Que.6 (a) Prove that the system of congruences , $x \equiv a(mod\ m)$; $x \equiv b(mod\ n)$ has solution iff $a \equiv b(mod\ (m, n))$. Also prove that system has unique solution with respect to modulo $[m, n]$. 4

(b) If $(a, m) = 1$ $a^{m-1} \equiv 1(mod\ m)$, and $a^n \not\equiv 1(mod\ m)$ for any proper divisor n of $m - 1$ then prove that m is prime . 3

(c) Solve the equation $12x + 15 \equiv 0(mod\ 45)$. 3

OR

Que.6 (a) State and prove Chinese remainder theorem. 4

(b) If a_1 , a_2 , a_3 , . . . , $a_{\Phi(m)}$ is RRS modulo m and $(a, m) = 1$,then prove that 3

(i) aa_1 , aa_2 , aa_3 , . . . , $aa_{\Phi(m)}$ is RRS mod m.
(ii) $aa_1 + b$, $aa_2 + b$, $aa_3 + b$, . . . , $aa_{\Phi(m)} + b$ is not RRS mod m , where b is any integer .

(c) If $m = p_1^{m_1} p_2^{m_2} p_3^{m_3} \dots p_k^{m_k}$,where all p_i are primes then prove that 3

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right).$$

—X—