

**MASTER OF SCIENCE EXAMINATION, 2023**

(2nd Year, 1st Semester)

**MATHEMATICS**

**UNIT - DSE 04 A30**

**[ NUMBER THEORY ]**

Time : 2 Hours

Full Marks : 40

Symbols have usual meanings, if not mentioned otherwise

Answer *Q. no. 1* and any *three* from the rest.

1. (a) Show that in any integral domain a prime element is irreducible.  
(b) Show that 3 is divisible by  $(1-\omega)^2$  in  $\mathbb{Z}[\omega]$ .  
(c) Show that  $\nu(n)$  is odd if and only if  $n$  is a square.  
(d) If  $n$  is not a prime, show that  $(n-1)! \equiv 0(n)$ , except when  $n=4$ . 2+2+3+3=10
  
2. (a) Show that the equation  $7x^2 + 2 = y^3$  has no solution in integers.  
(b) Solve the system of congruences  $x \equiv 1(7), x \equiv 4(9), x \equiv 3(5)$  with the help of Chinese Remainder Theorem.

[ Turn over

[ 2 ]

- (c) Let  $p$  be an odd prime. Show that  $a$  is a primitive root modulo  $p$  if and only if  $a^{(p-1)/q} \not\equiv 1 \pmod{p}$  for all prime divisors  $q$  of  $p-1$ . 2+3+5=10
3. (a) Suppose that  $a$  is a primitive root modulo  $p^n$ , where  $p$  is an odd prime. Show that  $a$  is a primitive root modulo  $p$ .
- (b) Find the solutions to the congruences  $x^3 \equiv 1 \pmod{19}$  and  $x^4 \equiv 1 \pmod{17}$ . 5+5=10
4. (a) Show that the minimal polynomial of  $\sqrt[3]{2}$  is  $x^3 - 2$  over  $\mathbb{Q}$ .
- (b) Use the Jacobi symbol to determine  $\left(\frac{215}{761}\right)$ ,  $\left(\frac{514}{1093}\right)$ , and  $\left(\frac{401}{757}\right)$ . 5+5=10
5. (a) Suppose that  $p$  is a prime with  $p \equiv 1 \pmod{3}$ . Prove that there are integers  $A$  and  $B$  such that  $4p = A^2 + 27B^2$ . If  $A \equiv 1 \pmod{3}$ , then prove that  $A$  is uniquely determined, and  $N(x^3 + y^3 = 1) = p - 2 + A$ .
- (b) Find the number of solutions to the equation  $x^3 + y^3 = 1$  in  $\mathbb{F}_p$  for  $p = 19, 37$ , and  $97$ . 5+5=10
6. (a) If  $\pi$  is a prime in  $\mathbb{D}$ , prove that  $x^3 \equiv 2 \pmod{\pi}$  is solvable if and only if  $\pi \equiv 1 \pmod{2}$ .

[ 3 ]

- (b) Suppose  $p$  is a rational prime such that  $p \equiv 1 \pmod{3}$ . Prove that  $x^3 \equiv 2 \pmod{p}$  is solvable if and only if there are integers  $C$  and  $D$  such that  $p = C^2 + 27D^2$ .
- (c) Show that
- (i)  $x^3 \equiv 2 \pmod{7}$  is not solvable, and
- (ii)  $x^3 \equiv 2 \pmod{31}$  is solvable. 3+4+3=10