

JK Lakshmipat University Jaipur
Institute of Engineering and Technology
End Term Examination, May 2025
B. Tech. (CSE), Semester VI, 2024-25

Roll No.....

AS1207: NUMBER THEORY

Time: 3 hours

Max. Marks: 40

Instructions to students:

1. All questions are compulsory.
2. Do not write anything other than your roll number on the question paper.
3. Calculators are not allowed.

-
- Q. 1.1** For any integer a , show that $\gcd(2a + 1, 9a + 4) = 1$. 1.0
(CO-1)
- Q. 1.2** Which of the following Diophantine equations cannot be solved and why? 1.0
(CO-1,3)
- i) $6x + 51y = 22$
- ii) $33x + 14y = 115$
- Q. 1.3** For $n > 3$, show that the integer $n, n + 2, n + 4$, cannot all be prime. 2.0
(CO-1,2)
- Q. 1.4** If $p \neq 5$ is an odd prime, prove that either $p^2 - 1$ or $p^2 + 1$ is divisible by 10. 2.0
(CO-1,2)
-
- Q. 2.1** A base b palindromic integer is an integer whose base b representation reads the same forward and backward. Show that every decimal palindromic integer with an even number of digits is divisible by 11. 2.0
(CO-1)
- Q. 2.2** Universal Product Codes (UPCs), typically 12 digits long, identify products as follows: the first digit denotes the category, the next five the manufacturer, the following five the product, and the last is a check digit. To calculate the check digit using the first 11 digits: 2.0
(CO-1,3)
- Add the digits in odd-numbered positions (starting from left) and multiply the sum by 3.
 - Add the digits in even-numbered positions to the result from step 1.
 - Find the check digit, which is the number that, when added to the total, makes it divisible by 10.
- Determine if the following 12-digit strings are valid UPCs:
- i) 0 38000 00127 5
- ii) 0 13900 00138 1
- Q. 2.3** For an odd prime, p , 3.0
- i) Show that positive integer a is its own inverse modulo p if and only if $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$. (CO-1,2)
- ii) Using Fermat's theorem, prove that
- $$1^{p-1} + 2^{p-1} + 3^{p-1} + \dots + (p-1)^{p-1} \equiv -1 \pmod{p}$$
-
- Q. 3.1** Determine whether each of the following arithmetic functions is totally multiplicative or multiplicative or both or neither: 1.0
(CO-4)
- i) $f(n) = n$ ii) $f(n) = \gcd(n, 6)$.
- Q. 3.2** Show that if n is the product of twin primes say $n = p(p + 2)$, then 2.0
(CO-4)
- $$\phi(n)\sigma(n) = (n + 1)(n - 3)$$

- Q. 3.3** Find all positive integers such that $\phi(n) = 12$. Be sure to prove that you have found all possibilities. **3.0**
(CO-1,4)
- Q. 3.4** If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, establish the following: **3.0**
(CO-1,4)
- i) $\sum_{d|n} \mu(d) \tau(d) = (-1)^r$
- ii) $\sum_{d|n} \mu(d) \phi(d) = (2 - p_1)(2 - p_2) \dots (2 - p_r)$
-
- Q. 4.1** Given that a has order 3 modulo p , where p is an odd prime, show that $a + 1$ must have order 6 modulo p . **1.0**
(CO-1,5)
- Q. 4.2** With the help of a primitive root of 7, find all incongruent primitive roots of 7^2 . **2.0**
(CO-5)
- Q. 4.3** Using mathematical induction, prove that if a is an odd integer, then for $k \geq 3$, $a^{2^{k-2}} \equiv 1 \pmod{2^k}$. **3.0**
(CO-1,5)
- Can you conclude about existence of primitive roots of 2^k , $k \geq 3$ on the basis of above result?
- Q. 4.4** In Elgamal cryptosystem, public key is given by (p, r, b) , where p is an odd prime, r is a primitive root of prime p and $b \equiv r^a \pmod{p}$, $0 \leq a \leq p - 1$. For $p = 13$, state the no. of incongruent possibilities for r and also find all of the them such that $r < 13$. For any one of value of r and a , find a public key for Elgamal cryptosystem for $p = 13$. **4.0**
(CO-1,5)
-
- Q. 5.1** Show that if a is a quadratic residue of the odd prime p , then a is not a primitive root of p . **1.0**
(CO-1,3)
- Q. 5.2** Using Quadratic Reciprocity Law, prove that if p and q are distinct odd primes, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv q \equiv 3 \pmod{4} \end{cases}$ **1.0**
(CO-1,3)
- Q. 5.3** Solve the quadratic congruence, $5x^2 + 6x + 1 \equiv 0 \pmod{23}$. **2.0**
(CO-3)
- Q. 5.4** State the Euler's criterion for quadratic residues and using the same, determine whether quadratic equation $x^2 \equiv -4 \pmod{19}$ is solvable or not and why. **2.0**
(CO-3)
- Q. 5.5** Evaluate the following Legendre symbols: **2.0**
(CO-1,3)
- i) $(71/73)$
- ii) $(-23/59)$
- Give proper reasons for your steps.
-
