



JK Lakshmi Pat University, Jaipur

Institute of Engineering and Technology

End Term Examination, May 2026

BTech, Even Semester, 2025-26

Roll No.....

AS1207: NUMBER THEORY

Time: 3 hours

Max. Marks: 35

Instructions to students:

1. Do not write anything other than your roll number on the question paper.
2. Calculator is not allowed.
3. Attempt all questions and justify your answers.
4. Notation: $\tau(n)$ is the number of positive divisors of n and $\sigma(n)$ is their sum, $\mu(n)$ is the Möbius function, $\phi(n)$ is the Euler's function.

Q.1	True/ False. (a) If $(a/p) = -1$ and $(b/p) = -1$, then the congruence $x^2 \equiv ab \pmod{p}$ has no solution. (b) If an odd prime p has a primitive root, then p^2 also has a primitive root. (c) $\mu(n)\mu(n+1) = 0$ for every positive integer $n \geq 1$. (d) The Mersenne number $M_p = 2^p - 1$ is always prime for every prime p.	4 x 0.25 (CO-1,2,5)
Q.2	Let $p \neq 3$ be an odd prime. The repunit R_n is defined as $R_n = \frac{10^n - 1}{9} = \underbrace{11 \dots 1}_{n \text{ digits}}$ Prove that if $p \mid R_n$, then the order of 10 modulo p must divide n.	1 (CO-5)
Q.3	If $n = p^k$ is a prime power, prove that $\phi(n) \cdot \sigma(n) = n^2 \left(1 - \frac{1}{p^2}\right)$ where $\sigma(n)$ is the sum of divisors function.	2 (CO-4)
Q.4	A reduced set of residues modulo n is a set of $\phi(n)$ integers that are coprime to n and pairwise incongruent modulo n. Let $a_1, a_2, \dots, a_{\phi(n)}$ be reduced set of residues modulo n, then show that $\sum_{i=1}^{\phi(n)} a_i \equiv 0 \pmod{n}.$ (Hint: $\gcd(a, n) = \gcd(n - a, n)$)	2 (CO-1,4)
Q.5	Evaluate the following Legendre symbols: (a) $\left(\frac{26}{41}\right)$ (b) If p and $q = 2p + 1$ are odd primes with $p \equiv 1 \pmod{4}$, determine the value of $\left(\frac{2}{q}\right)$.	2 (CO-3)
Q.6	(a) Find all positive integers n such that $\phi(n) = 4$. (b) Prove that $\tau(n) = 2^r$ for square-free n with r distinct prime factors.	2+1 (CO-4)
Q.7	Let p be an odd prime. Define $M = \left(\frac{p-1}{2}\right)!$ (i.e., the factorial of $\frac{p-1}{2}$). Using the Wilson's theorem, prove that $M^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$ Hence deduce, if $p \equiv 1 \pmod{4}$, then M is a solution of the congruence $x^2 \equiv -1 \pmod{p}$.	3 (CO-1,2,3)

Q.8	(a) Use Euler's theorem to show that for all integers $n \geq 0$, $15 \mid 7^{4n+2} - 4$. (b) Show that if p and q are distinct odd primes with $p-1 \mid q-1$ and $\gcd(a, pq) = 1$, then $a^{q-1} \equiv 1 \pmod{pq}$.	2+2 (CO-1)
Q.9	Determine all positive integers n for which the decimal representation of $n!$ ends in exactly 7 zeros. Justify your answer using the formula $\sum_{k \geq 1} [n/5^k]$ for the exponent of 5 in $n!$, where, $[x]$ is the greatest integer less than or equal to x .	2 (CO-1)
Q.10	Solve the quadratic congruence $2x^2 + 3x + 1 \equiv 0 \pmod{13}$ and find the two incongruent solutions modulo 13.	3 (CO-3)
Q.11	Fermat's primality test declares an integer n composite if there exists an integer a coprime to n such that $a^{n-1} \not\equiv 1 \pmod{n}$. A composite integer that escapes this test for a particular base a is called a pseudoprime to base a. (a) Show that 341 is a pseudoprime to base 2, i.e., Fermat's test with $a = 2$ fails to detect that 341 is composite. (b) Show that Fermat's test with base $a = 3$ correctly identifies 341 as composite and conclude that 341 is not a Carmichael number.	2 (CO-1,2)
Q.12	(a) Given that 2 is a primitive root of 19. Find all positive integers less than 19 having order 3 modulo 19. (b) Let p be an odd prime and r a primitive root modulo p. Prove that an integer a coprime to p is a quadratic residue modulo p if and only if $a \equiv r^k \pmod{p}$ for some even integer k. Given that 3 is a primitive root modulo 7, use this result to list the quadratic residues of 7.	2+3 (CO-4,5)
Q.13	Consider the eight-digit bank identification number $a_1 a_2 \dots a_8$, which is followed by a ninth check digit a_9 chosen to satisfy the congruence $a_9 \equiv 7a_1 + 3a_2 + 9a_3 + 7a_4 + 3a_5 + 9a_6 + 7a_7 + 3a_8 \pmod{10}$ (a) Obtain the check digits that should be appended to the two numbers 55382006. (b) The bank identification number 237$a_4$18538 has an illegible fourth digit. Determine the value of the obscured digit.	2 (CO-1,4)
Q.14.	Theorem. Let p be an odd prime. Then the product of all primitive roots modulo p is congruent to 1 modulo p for $p > 3$, while for $p = 3$ it is not congruent to 1. Complete the following proof of the above theorem by filling in the blanks. Proof. Case 1: $p = 3$. The only primitive root modulo 3 is _____ (blank 1). Consequently, the product of all primitive roots modulo 3 equals _____ modulo 3 (blank 2), which is not congruent to 1. Case 2: $p > 3$ Let g be a primitive root modulo p. Then $\text{ord}_p(g) = ______ (blank 3)$. Every primitive root modulo p can be written uniquely in the form g^k with $0 < k < p-1$ and $\gcd(k, ______) = 1 (blank 4)$. Therefore, the total number of primitive roots modulo p is $\phi(______) (blank 5)$.	3 (CO-4,5)

Now take any primitive root $r = g^k$. Its modular inverse r^{-1} is g^{p-1-k} , it will also be a primitive root because $\gcd(p-1-k, p-1) = 1$. Thus, we can attempt to pair each primitive root with its inverse.

If $r = r^{-1}$, then $r^2 \equiv 1 \pmod{p} \Rightarrow r \equiv 1 \text{ or } -1$.

The order of 1 is 1 and $\text{ord}_p(-1) = \underline{\hspace{1cm}}$ (blank 6).

Since $p > 3$, we have $p-1 > \underline{\hspace{1cm}}$ (blank 7); consequently, neither 1 nor -1 can have order $p-1$, which is the order required for a primitive root. Hence $\underline{\hspace{1cm}}$ (blank 8) primitive root equals its own inverse.

Consequently, the set of all primitive roots form disjoint pairs $\{r, r^{-1}\}$, each pair satisfying $r \cdot r^{-1} \equiv \underline{\hspace{1cm}} \pmod{p}$ (blank 9).

For $p > 3$, the number $\phi(p-1)$ is always $\underline{\hspace{1cm}}$ (even / odd) (blank 10).

Therefore the total product of all primitive roots is

$$\prod_{\substack{1 \leq k \leq p-2 \\ \gcd(k, p-1)=1}} g^k \equiv 1^{\frac{\phi(p-1)}{2}} \equiv \underline{\hspace{1cm}} \pmod{p} \text{ (blank 11) .}$$

Conclusion: For every odd prime $p > 3$, the product of all primitive roots modulo p is congruent to $1 \pmod{p}$. For $p = 3$, the product is congruent to $\underline{\hspace{1cm}} \pmod{3}$ (blank 12).

-----END-----

