

3 copy

C 21073

(Pages : 3)

Name.....

Reg. No.....

SIXTH SEMESTER B.Sc. DEGREE EXAMINATION, MARCH 2017

(CUCBCSS-UG)

Mathematics

MAT 6B 12—NUMBER THEORY AND LINEAR ALGEBRA

Time : Three Hours

Maximum : 120 Marks

Section A

*Answer all the twelve questions.
Each question carries 1 mark.*

1. Find gcd (143,227).
2. Give an example of linear Diophantine equation in two variables.
3. Write two integers a and b such that a is incongruent to b modulo 5.
4. State the Fundamental Theorem of Arithmetic.
5. Define pseudoprime. Give an example of a Pseudoprime number.
6. Find $\tau(12)$.
7. Define Euler's Phi function.
8. Define subspace of a vector space.
9. Define dimension of a vector space.
10. Check whether the following map is linear. $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ defined by $f(x,y,z) = (z, -y,x)$.
11. Define the rank of a linear map.
12. State the dimension theorem.

(12 × 1 = 12 marks)

Section B

*Answer any ten questions from among the questions 13 to 26.
Each question carries 4 marks.*

13. Use the Euclidean Algorithm to obtain integers x and y satisfying $\gcd(56,72) = 56x + 72y$.
14. Find all the integer solutions of the Diophantine equation $6x + 15y = 22$.
15. Prove that the linear Diophantine equation $ax + by = c$ has an integer solution if and only if $d \mid c$ where $d = \gcd(a, b)$.
16. Prove that $\sqrt{3}$ is irrational.
17. For arbitrary integers a and b prove that $a \equiv b \pmod{n}$ if and only if a and b leave the same remainder when divided by n.
18. Find the remainder when 2^{50} is divided by 7.

Turn over

19. If p and q are distinct primes with $a^p \equiv a \pmod{q}$ and $a^q \equiv a \pmod{p}$, then prove that $a^{pq} \equiv a \pmod{pq}$.
20. Show that $18! \equiv -1 \pmod{437}$.
21. If p is a prime and $k > 0$, then show that $\phi(p^k) = p^k \left(1 - \frac{1}{p}\right)$.
22. Prove that the monomials $1, x, \dots, x^n$ form a basis for $\mathbb{R}_n[X]$.
23. Show that a line in \mathbb{R}^3 that does not pass through the origin cannot be a subspace of \mathbb{R}^3 .
24. Show that $(1,1,0,0), (-1, -1,1,2), (1, -1,1,3), (0,1, -1, -3)$ is a basis of \mathbb{R}^4 .
25. If $f: V \rightarrow W$ is linear, then prove that the following statements are equivalent: (1) f is injective; (2) $\text{Ker } f = \{0\}$.
26. The mapping $f: \mathbb{R}^2 \rightarrow \mathbb{R}^3$ given by $f(a, b) = (a + b, a - b, b)$ is linear. (10 × 4 = 40 marks)

Section C

Answer any six questions from among the questions 27 to 35.
Each question carries 7 marks.

27. Given integers a and b , not both of which are zero, prove that there exists integers x and y such that $\text{gcd}(a, b) = ax + by$.
28. Prove that $\text{gcd}(a, b) \text{ lcm}(a, b) = ab$, where a and b are positive integers.
29. Prove that there are infinite number of primes.
30. Let p be a prime number and suppose that $p \nmid a$, then prove that $a^{p-1} \equiv 1 \pmod{p}$.
31. Derive Legendre formula for $n!$
32. If V is a vector space with $\dim V = 10$ and X, Y are subspaces of V with $\dim X = 8$ and $\dim Y = 9$, then find the smallest possible value of $\dim(X \cap Y)$.
33. Let V be a finite-dimensional vector space. If G is a finite spanning set of V and if I is a linearly independent subset of V such that $I \subseteq G$ then there is a basis B of V such that $I \subseteq B \subseteq G$.
34. Let V and W be vector spaces over a field F . If v_1, \dots, v_n is a basis of V and w_1, \dots, w_n are elements of W (not necessarily distinct) then show that there is a unique linear mapping $f: V \rightarrow W$ such that $f(v_i) = w_i, i = 1, 2, 3, \dots, n$.
35. Show that the linear mapping $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ given by $f(x, y, z) = (x + y + z, 2x - y - z, x + 2y - z)$ is both surjective and injective. (6 × 7 = 42 marks)

Section D

Answer any **two** questions from among the questions 36 to 38.
Each question carries 13 marks.

36. State and Prove Division Algorithm. Illustrate with an example.
37. State and prove Chinese Remainder Theorem.
38. Let V be a vector space that is spanned by the finite set $G = \{v_1, \dots, v_n\}$. If $I = \{w_1, \dots, w_m\}$ is a linearly independent subset of V then show that $m \leq n$.

(2 × 13 = 26 marks)