C 40188 **(Pages : 3)** **Name.......................................**

Reg. No...................................

SXTH SEMESTER (CUCBCSS–UG) DEGREE EXAMINATION, MARCH 2023

Mathematics

MAT 6B 12—NUMBER THEORY AND LINEAR ALGEBRA

(2017–2018 Admissions)

Time : Three Hours Maximum : 120 Marks

Section A

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

1. Define greatest common divisor of a and b.
2. State Euclid's lemma.
3. Examine whether the Diophantine equation $6x + 51y = 22$ has an integer solution.
4. If p is a prime and $p \mid ab$, show that $p \mid a$ or $p \mid b$.
5. Define Euclidean number. List the first five Euclidean numbers.
6. State Wilson's Theorem.
7. Find $\phi(360)$.
8. Define Vector Space.
9. Give an example to show that union of two subspaces need not be subspace.
10. Check whether the map $f : \mathbb{R}^3 \to \mathbb{R}^3$ defined by $f(x, y, z) = (2x, y - 2, 4y)$ is linear. Justify your claim.
11. State the Dimension theorem.
12. When we say that a linear map is an isomorphism. Give an example for an isomorphism ?

(12 × 1 =12 marks)

Section B

Answer any **ten** *out of fourteen questions.*
Each question carries 4 *marks.*

13. Prove that $3a^2 - 1$ is never a perfect square.
14. If $\gcd(a, b) = d$, prove that $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Turn over

15. Use the Euclidean Algorithm to find $\gcd(12378, 3054)$.

16. Prove that every integer $n > 1$ can be expressed as a product of primes.

17. Prove that the number $\sqrt{3}$ is irrational.

18. Using Sieve of Eratosthenes find all primes not exceeding 100.

19. Show that 41 divides $2^{20} - 1$.

20. Let $N = a_m 10^m + a_{m-1} 10^{m-1} + \ldots + a_1 10 + a_0$ be the decimal expansion of the positive integer $N, 0 \le a_k < 10$, and let $S = a_0 + a_1 + \ldots + a_m$. Prove that $9 \mid N$ if and only if $9 \mid S$.

21. Find the remainder when 15 ! is divided by 17.

22. Prove that every line through the origin is a subspace of $\mathbb{R}^2$.

23. If the vector space V has a finite basis B then show that every basis of V is finite and has the same number of elements as B.

24. Let $f : V \to W$ be linear. Prove that if X is subspace of V then $f^{\to}(X)$ is a subspace of W.

25. Find *Im f* and *Ker f* when $f : \mathbb{R}^3 \to \mathbb{R}^3$ is given by $f(a,b,c) = (a+b, b+c, a+c)$.

26. Let $f : V \to W$ be a linear map. Prove that f is injective if and only if $\ker f = \{0\}$.

(10 × 4 = 40 marks)

Section C

Answer any **six** *out of nine questions.*
Each question carries 7 *marks.*

27. If a and b are given integers, not both zero, prove that the set $T = \{ax + by : x, y \text{ are integers}\}$ is precisely the set of all multiples of $d = \gcd(a,b)$.

28. Prove that $\gcd(a,b)\, lcm(a,b) = ab$, where a and b are positive integers.

29. Find the complete solution of the linear Diophantine equation $172x + 20y = 1000$. Also find solutions in positive integers if they exist.

30. Using Chinese Remainder Theorem, solve the system of congruences $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$.

31. Let p be a prime and suppose that $p \mid a$. Prove that $a^{p-1} \equiv 1 (\text{mod } p)$.

32. (a) Prove that $\langle S \rangle = \text{span } S$. (4 marks)

(b) Show that $\{(1,1,1), (1,2,3), (2,-1,1), (2,-1,1)\}$ is a basis of $\mathbb{R}^3$. (3 marks)

33. If the vector space V has a finite basis B then show that every basis of V is finite and has the same number of elements as B.

34. Let V and W be vector spaces over a field F. If $\{v_1, v_2, \ldots, v_n\}$ is a basis of V and $w_1, w_2, \ldots, w_n$ are elements of W then show that there is a unique linear mapping $f : V \to W$ such that $f(v_i) = w_i$ for $i = 1, 2, \ldots, n$.

35. If $f : \mathbb{R}^3 \to \mathbb{R}^3$ is a linear map such that $f(1,1,1) = (1,1,1)$, $f(1,2,3) = (-1,-2,-3)$, $f(1,1,2) = (2,2,4)$, then find $f(x,y,z)$ for all $(x,y,z) \in \mathbb{R}^3$.

(6 × 7 = 42 marks)

Section D

Answer any **two** *out of three questions.*
Each question carries 13 *marks.*

36. (a) Prove that the quadratic congruence $x^2 + 1 \equiv 0 (\text{mod } p)$, where p is an odd prime, has a solution if and only if $p \equiv 1 (\text{mod} 4)$.

(10 marks)

(b) Prove that If $n > 1$, then the sum of the positive integers less than n and relatively prime to n is $\frac{1}{2} n \phi(n)$.

(3 marks)

37. (a) State and Prove Division Algorithm. (10 marks)

(b) Prove that square of any integer is either $3k$ or $3k + 1$. (3 marks)

38. Show that the linear mapping $f : \mathbb{R}^3 \to \mathbb{R}^3$ given by $f(x,y,z) = (x+z, x+y+2z, 2x+y+3z)$ is neither surjective nor injective.

(3 × 13 = 39 marks)