D 93265 (Pages : 3) Name.....

Reg. No.....

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, DECEMBER 2015

(CCSS)

Mathematics

MAT 1C 05—NUMBER THEORY

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries 4 *marks.*

I. 1 Let p be a prime and $f(x)$ a polynomial with integer coefficients. What can be said about the number of roots of $f(x)$ modulo p ? Prove your answer.

2 Let p be a prime and d a natural number with $d \mid p-1$. Prove that the equation $x^d \equiv 1 \pmod{p}$ has exactly d distinct solutions modulo p. Indicate clearly where your proof uses the hypothesis that p is a prime.

3 Use the Euclidean Algorithm to determine all the solutions of :

$32x \equiv 20 \pmod{108}$.

4 Let $d_1, d_2, \ldots\ldots, d_k$ be all the factors of a positive integer n including 1 and n. Find the value of $\frac{1}{d_1}+\frac{1}{d_2}+\ldots\ldots+\frac{1}{d_k}$, given that , $d_1+ + \ldots. d_k = 72$.

5 Find the last nonzero digit from the left in the decimal value of 234!.

6 If $n > 1$, prove that the sum $\sum_{k=1}^{n}\frac{1}{k}$ is not an integer.

7 If gcd $(a, b) = 1$ and $ab = c^n$, prove that $a = x^n$ and $b = y^n$ for some x and y.

8 Let $d(n)$ denotes the number of positive divisors of n. Prove that $d(n)$ is odd if, and only if, n is a square.

9 Prove that there are infinitely many primes of the form $4n + 3$.

10 Let s_n denote the n^{th} partial sum of the series $\sum_{r=1}^{\infty}\frac{1}{r(r+1)}$. Prove that for every integer $k > 1$ there exist integers m and n such that $s_m - s_n = \frac{1}{k}$.

Turn over

11 Find all those odd primes p for which 2 is a quadratic residue and those for which it is a non residue.

12 Consider the elliptic curve $y^2 = x^3 - 2$. Find a rational point (both x and y are rational) on the curve other than $(3, \pm 5)$.

$(12 \times 4 = 48$ marks)

Part B

Answer **either** *A* **or** *B of each question.*
Each question carries 8 *marks.*

II. A (p) Prove that a number of the form $10x + y$ is divisible by 7 if and only if $x - 2y$ is divisible by 7. Using this method prove that 4580247 is divisible by 7.

(q) Prove the Wilson's Theorem and its converse. Can we use Wilson's theorem for checking primarily of an integer ? Explain why or why not.

B (r) Find an integer n such that $1^2 + 2^2 + 3^2 + ... + n^2$ is a perfect square.

(s) Let p be an prime, $p \geq 5$, and write $1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{p} = \frac{r}{ps}$. Prove that $p^3 \mid (r - s)$.

III. A (p) Let $f(x) = x^2 + x + 41$. Find the smallest integer $x \geq 0$ for which $f(x)$ is composite.

(q) Find a lower and upper bound for n^{th} prime p_n.

B (r) Let p be an odd prime. Prove that

(i) $1^2 \cdot 3^2 \cdot 5^2 ..... (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$ and

(ii) $2^2 \cdot 4^2 \cdot 6^2 ..... (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.

(s) State and prove Fermat's little theorem. Is the converse true ? Justify your answer.

IV. A (p) Design an efficient algorithm to generate a random number n, which is a quadratic non-residue modulo p, where p is a prime.

(q) Solve $x^2 \equiv 211 \pmod{257}$, given that 3 is a quadratic non-residue of the prime 257.

B. (r) Using Fermat little theorem or otherwise, solve $x^3 \equiv 211 \pmod{257}$.

(s) State and prove Gauss lemma for quadratic character of n with respect to the prime p.

V. A. (p) Decrypt the cipher text message OZKFZ XPPDDA created by an affine cipher $C = 5P + 11 \pmod{26}$.

(q) Define Jacobi's symbol $\left(\frac{P}{Q}\right)$, where P and Q are odd integers. Explain how you can compute Legendre symbol by using Jacobi's symbol. What are the advantageous of your method ?

B. (r) Describe an indistinguishable data transfer mechanism by using Jacob symbol. Show how you can encrypt a bit (0 *or* 1).

(s) Explain any one Public key cryptosystem with an example.

(4 × 8 = 32 marks)

D 93263 (Pages : 3) Name.....

Reg. No.....

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, DECEMBER 2015

(CCSS)

Mathematics

MAT 1C 03—LINEAR ALGEBRA

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *questions.*
Each question carries **4** *marks.*

1. Let F be a field and F^n, the set of all n-tuples $(x_1, x_2, \ldots x_n)$, $n \geq 2$. Is F^n a vector space, if so what is the dimension of F^n ? Is the set of all n-tuples with $x_1 = 1 + x_2$ a subspace of F^n ? Justify your answer.

2. Show that the vectors $(1, 0, -1), (1, 2, 1), (0, -3, 2)$ is a basis for R^3.

3. Let B and B′ be two ordered bases of an n-dimensional vector space over a field F. Show that there exists a unique invertible $n \times n$ matrix P such that

$$[\alpha]_B = P\,[\alpha]_{B'}.$$

where $[\alpha]_B, [\alpha]_{B'}$ represents the coordinate matrix of α relative to the ordered bases B and B′ respectively.

4. Let V be a vector space over a field F. Suppose that there are finite number of vectors $\alpha_1, \ldots, \alpha_r$ in V which spans V. Prove that V is finite dimensional.

5. Let $T : C \to C$ given by $T(z) = iz$ is T linear. Justify your answer.

6. Let A be an 2×2 matrix over a field F. Prove that *det* $(I + A) = I +$ *det* A if and only if *trace* $(A) = 0$.

7. Let $A = \begin{pmatrix} 2 & 3 \\ -1 & 1 \end{pmatrix}$. Find the characterstic values of A.

Turn over

8. State true or false with justification. If a digonalizable operator has only characterstic values 0 and 1, then it is a projection.

9. Let V be a vector space and E and a projection of V, then is E always digonalizible ? Justify your answer.

10. If T is a linear operator on the n-dimensional vector space V having n-distinct characterstic values then T is diagonalizable. Is this statement true ? Justify your answer.

11. Let W be a k-dimensional subspace of an n-dimensional vector space V, then show that W is the intersection of $(n-k)$ hyper sub-spaces in V.

12. Show that every matrix A such that $A^2 = A$ is similar to a digonal matrix.

(12 × 4 = 48 marks)

Part B

Answer either A **or** *B of each question.*
Each question carries 8 *marks.*

II. A. (a) Let V be a vector space over a field F, then define a subspce of V and show that intersection of any family of subpaces of V is subspace of V.

(b) Let W be a subspace of C^3 spanned by $\alpha_1 = (1, 0, i)$ and $\alpha_2 = (1+i, 1, -1)$ show that α_1 and α_2 forms a basis for W.

B. (a) If W_1 and W_2 are finite dimensional subspaces of a vector space V, then show that $W_1 + W_2$ is finite dimensional and

$$\dim W_1 + \dim W_2 = \dim (W_1 \cap W_2) + \dim (W_1 + W_2).$$

III. A. (a) Let V and W be vector spaces over a field F and let T be a linear transformation from V into W. Suppose V is finite dimensional then show that

$$\text{rank } (T) + \text{nullity } (T) = \dim V.$$

(b) Let T be a linear transformation from V into W. Show that T is non-singular if and only if T carries each linearly independant subset of V onto a linearly independent subset of W.

B. (a) Compute a matix representation of the differential operator D acting on the vector space V of all polynomial functions from R into R of degree three of less.

(b) If f is a non-zero linear functional on a vector space V, then show that the null space of f is a hyperspace in V.

IV. A. Let T be the linear operator on R^3 which is represented in the standard ordered basis by the matrix.

$$A = \begin{pmatrix} 5 & -6 & -6 \\ -1 & 4 & 2 \\ 3 & -6 & -4 \end{pmatrix}.$$

Find the characteristic values and the dimension of the space of characteristic vectors. Is T diagonalizable ? Justify your answer.

B. State and prove Cayley-Hamilton theorem.

V. A. Let T be a linear operator on a finite dimensional space V. If T is diagonalizable and if $c_1, \ldots . c_k$ are distinct characterstic values of T, then show that there exists linear operators $E_1, \ldots . , E_k$ on V such that :

(i) $T = c_1 E_1 + \ldots . . + c_k E_k$.

(ii) $I = E_1 + \ldots . . + E_k$.

B. (a) Let V be a vector space and $(|)$ an inner product on V, then show that $(0 \mid \beta) = 0$ for all β in V.

(b) Let V be an inner product space, then for any vectors $\alpha, \beta \in V$. and any scalar c, show that

(i) $\|\alpha\| = |c| \, \|\alpha\|$.

(ii) $\|\alpha\| > 0$ for $\alpha \neq 0$.

(iii) $\|\alpha + \beta\| \leq \|\alpha\| + \|\beta\|$.

(4 × 8 = 32 marks)

D 93262 (Pages : 3) Name.....

Reg. No.....

FIRST SEMESTER M.Sc. DEGREE EXAMINATION, DECEMBER 2015

(CCSS)

Mathematics

MAT 1C 02—REAL ANALYSIS—I

Time : Three Hours Maximum : 80 Marks

Answer **all** *questions from Part A.*
Each question carries 4 *marks.*
From Part B answer **either** *A* **or** *B of each question.*
Each question carries 8 *marks.*

Part A

I. 1 Prove that a set E is open if and only if its complement is closed.

2 Prove that every bounded infinite subset of R^k has a limit point in R^k.

3 Let k be a positive integer. If $\{I_n\}$ is a sequence of k-cells such that $I_n \supset I_{n+1}, n = 1,2,3,\ldots$, prove that $\bigcap_1^\infty I_n$ is not empty.

4 Suppose f is a continuous mapping of a metric space X into a metric space Y. Prove that $f(E)$ is connected if E is a connected subset of X.

5 Let E be a bounded set and non-compact set in R^1. Show that there exists a continuous function on E which is not uniformly continuous.

6 If $C_0 + \frac{C_1}{2} + \ldots + \frac{C_{n-1}}{n} + \frac{C_n}{n+1} = 0$ where $C_0, \ldots, C_n$ are real constants, prove that the equation $C_0 + C_1 x + \ldots + C_{n-1}x^{n-1} + C_n x^n = 0$ has at least one real root between 0 and 1.

7 Prove that $f \in R(x)$ on $[a, b]$ if f is continuous on $[a, b]$.

8 Prove that $L(p,f,\alpha) \le L(p^*,f,\alpha)$ if p^* is a refinement of p.

9 Let $f_n(x) = \frac{\sin nx}{\sqrt{n}}$ on R. Does f_n converges uniformly to f ? Does f_n converges to f' ? Justify your answers.

10 If $I(x)=\begin{cases}0, & x\le 0\\ 1, & x>0\end{cases}$ if $\{x_n\}$ is a sequence of distinct points of (a, b) and if $\Sigma|C_n|$ converges, prove that the series $f(x)=\sum_{n=1}^{\infty} C_n I(x-x_n)\ a\le x\le b$ converges uniformly, and that f is continuous for every $x\neq x_n$.

11 Let $f_n(x)=\begin{cases}0, & x<\frac{1}{n+1}\\ \sin^2\frac{\pi}{x}, & \frac{1}{n+1}\le x\le\frac{1}{n}\\ 0, & \frac{1}{n}<x\end{cases}$, show that $\{f_n\}$ converges to a continuous function, but not uniformly.

12 Suppose $\mathcal{A}$ is an algebra of functions on a set E, $\mathcal{A}$ separates points on E and $\mathcal{A}$ vanishes at no point of E. Suppose x_1, x_2 are distinct points of E, and C_1, C_2 are constants. Prove that $\mathcal{A}$ contains a function f such that $f(x_1)=c_1, f(x_2)=c_2$.

(12 × 4 = 48 marks)

Part B

II. A (a) Prove that compact subsets of metric spaces are closed.

(b) Prove that $F\cap K$ is compact if F is closed and K is compact.

Or

B Suppose $Y\subset X$, where X is a metric space, prove that a subset E of Y is open relative to Y if and only if $E=Y\cap G$ for some open subset G of X.

III. A Prove that a mapping f of a metric space X into a metric space Y is continuous on X if and only if $f^{-1}(V)$ is open in X for every open set V in Y.

Or

B State and prove Taylor's theorem.

IV. A If $\bar{f}$ maps $[a, b]$ into R^k and if $\bar{f}\in\mathcal{R}(\alpha)$ for some monotonically increasing function α on $[a, b]$, prove that $|\bar{f}|\in R(\alpha)$ and $\left|\int_a^b \bar{f}\,d\alpha\right|\le\int_a^b|\bar{f}|\,d\alpha$.

Or

B (a) Prove that $f \in R(x)$ on $[a, b]$ if and only if for every $\varepsilon > 0$ there exists a partition p such that $U(p,f,\alpha) - L(p,f,\alpha) < \varepsilon$.

(b) Suppose $f \geq 0$, f is continuous on $[a, b]$ and $\int_a^b f(x)\,dx = 0$. Prove that $f(x) = 0$ for all $x \in [a,b]$.

V. A Let K be compact and $\{f_n\}$ be a sequence of continuous functions on K which converges pointwise to a continuous function f on K and $f_n(x) \geq f_{n+1}(x)$ for all $x \in K$. Prove that f_n converges to f uniformly on K.

Is this result true if we delete the condition that K is compact ?

Or

B State and prove Stone-Weierstrass theorem.

(4 × 8 = 32 marks)