C 6764

(Pages : 2)

Name.....................................

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

SECOND SEMESTER M.Sc. DEGREE EXAMINATION, JULY 2010

Mathematics

Paper X—NUMBER THEORY

(2003 admission onwards)

Time : Three Hours

Maximum : 80 Marks

Part A

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

1. (a) Determine all integers n such that $\varphi(n) = 8$.

   (b) Prove the converse of Wilson's theorem :

   If $(n-1)! + 1 \equiv 0 \pmod{n}$, then n is a prime if $n > 1$.

   (c) Prove that $[x] + \left[x + \frac{1}{2}\right] = [2x]$.

   (d) Find all solutions $\binom{x}{y}$ modulo 29, writing x and y as non-negative integers less than 29.

   $9x + 20y \equiv 10 \bmod 29$

   $16x + 13y \equiv 21 \bmod 29$.

(4 × 4 = 16 marks)

Part B

Answer any **four** *questions without omitting any unit.*
Each question carries 16 *marks.*

UNIT I

2. (a) Prove that the Dirichlet multiplication is commutative and associative.

   (b) Define the Mangoldt function $\wedge(n)$. Show that $\sum_{d/n} \wedge(d) = \log_n$ if $n \geq 1$.

   (c) Let $f(n) = \left[\sqrt{n}\right] - \left[\sqrt{n-1}\right]$. Prove that f is multiplicative but not completely multiplicative.

3. (a) If $x \geq 1$, prove that $\sum_{n \leq x} \frac{1}{n} = \log x + C + 0\left(\frac{1}{x}\right)$ where C is the Euler's constant.

   (b) State and prove Abel's identities.

Turn over

4. (a) Prove that for an integer $n \geq 2$, we have $\frac{1}{6}\frac{n}{\log n} < \pi(n)$.

(b) Define the functions M(x) and H(x). Prove that $\lim_{x \to \infty}\left(\frac{M(x)}{x} - \frac{H(x)}{x \log x}\right) = 0$.

UNIT II

5. (a) Assume $(a, m) = 1$. Then prove that the linear congruence

$$ax \equiv b \pmod{m}$$

has exactly one solution.

(b) State and prove the Chinese remainder theorem.

(c) Prove that $5n^3 + 7n^5 \equiv 0 \pmod{12}$ for all integers n.

6. (a) Let p be an odd prime. Prove that for all n, we have $(n/p) \equiv n^{(p-1)/2} \pmod{p}$ deduce that the Legendre's function (n/p) is a completely multiplicative function of n.

(b) Determine whether 222 is a quadratic residue on nonresidue of the prime 1999.

7. (a) State and prove Gauss' lemma.

(b) Let m be the number defined in Gauss' lemma show that

$$m \equiv \sum_{t=1}^{(p-1)/2}\left[\frac{t_n}{p}\right] + (n-1)\frac{(p^2-1)}{8} \pmod{2}$$

UNIT III

8. (a) Describe encryption using encephering matrices. Illustrate with an example.

(b) In the 27-letter alphabet (with blank = 26), use the affine enciphering transformation with Key $a = 13, b = 9$ to encepher the message "HELP ME".

9. (a) Find the inverse of $\begin{pmatrix} 1 & 3 \\ 4 & 3 \end{pmatrix}$ mod 29.

(b) Explain the importance and methods of authentication in public key cryptography.

10. (a) Explain the RSA cryptosystem. Illustrate with an example.

(b) Describe an algorithm for finding discrete logs in finite fields.

(Pages: 2)

2

Name ....
Reg. No ....

Second Semester M. Sc. Degree Examination, July 2010
(Mathematics)
Paper VIII–Topology I
(2003 admissions onwards)

Time: 3 Hrs

Max. Marks: 80

Part A

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

I (a) Let X be any set and let

$$\tau = \{A \subset X : X - A \text{ is finite}\} \cup \{\phi\}.$$

Is τ a topology on X? Justify your answer.

(b) Let X, Y be topological spaces, $f : X \to Y$ be a function and let $\text{Gr}(f) = \{(x, f(x)) : x \in X\}$. If f is continuous, then prove that $\text{Gr}(f)$ is homeomorphic to X.

(c) Prove that a set is closed if and only if it contains its boundary

(d) Prove that the continuous image of a connected space is connected.

($4 \times 4 = 16$ marks)

Part B

Answer any **four** questions without omitting any unit.
Each question carries 16 marks.

UNIT I

II (a) Let $(X; d)$ be a metric space. Prove that

(i) the empty set $\emptyset$ and the set X are open,

(ii) the union of any family of open sets is open,

(iii) the intersection of any finite number of open sets is open.

(b) Prove that every open cover of a second countable space has a countable subcover.

III (a) Let X be a set, τ a topology on X and S a family of subsets of X. Prove that S is a subbase for τ if and only if S is generated by τ

(b) Let X be a topological space and $A \subset X$. Prove that A is closed if and only if $\overline{A} = A$.

IV (a) Prove that composition of continuous functions is continuous.

(b) Let X be a topological space and $Y \subset X$. Prove that the closed subsets of Y are intersections of closed subsets of X with Y.

UNIT II

V (a) Prove that the product topology is the weak topology determined by the projection functions.

(b) Prove that every closed bounded interval of $\mathbb{R}$ is compact.

VI (a) Prove that every continuous real valued function on a compact space is bounded and attains its extrema.

(b) Let X be a Lindelöff space and $A \subset X$ be closed in X. Prove that A is Lindelöff in its relative topology.

VII (a) Prove that every path connected space is connected.

(b) Prove that the topological product of finite number of connected spaces is connected.

UNIT III

VIII (a) Prove that a topological space X is a T_1-space if and only if each singleton set $\{x\}$ is closed in X.

(b) Prove that every metric space is T_4

IX (a) Prove that every regular Lindelöff space is normal.

(b) Prove that regularity is a hereditary property in topological spaces.

X (a) Prove that all T_4 spaces are Tychnoff.

(b) If a topological space X has the property that for any two disjoint closed subsets A, B of X there exists a continuous function $f : X \to [0,1]$ taking value 0 at all points of A and the value 1 at all points of B, then prove that X is normal.

(Pages: 2)

Name ....

Reg. No ....

Second Semester M. Sc. Degree Examination, July 2010
(Mathematics)
Paper VII–Real Analysis–II
(2003 admissions onwards)

Time: 3 Hrs   Max. Marks: 80

Part A

Answer all questions. Each question carries 4 marks

I (a) Prove that the outer measure m^* is translation invariant.

(b) Prove that the cantor set is of measure zero.

(c) Let f be a nonnegative measurable function. Show that $\int f = 0$ implies $f = 0$ *a.e.*.

(d) Let X be a vector space and let $\dim X = n$. Prove that a set E of n vectors in X spans X if and only if E is independent.

Part B

Answer any **four** questions without omitting any unit.
Each question carries 16 marks.

UNIT I

II (a) Let Ω be the set of all invertible linear operators on $\mathbb{R}^n$. Prove that Ω is an open subset of $L(\mathbb{R}^n)$ and the mapping $A \to A^{-1}$ is continuous.

(b) Let X be a complete metric space and φ be a contraction mapping of X into X. Prove that there exists one and only one $x \in X$ with $\varphi(x) = x$.

III (a) Let E be an open subset of $\mathbb{R}^n$ and let f be a mapping of E into $\mathbb{R}^m$. Prove that f is continuously differentiable in E if and only if the partial derivatives $D_j f_i$ exist and are continuous on E for $1 \le i \le m$, $1 \le j \le n$.

(b) Prove that a linear operator A on $\mathbb{R}^n$ is invertible if and only if $\det[A] \neq 0$.

IV (a) State and prove implicit function theorem.

(b) Let $f = (f_1, f_2)$ be the mapping of $\mathbb{R}^2$ into $\mathbb{R}^2$ given by $f_1(x,y) = e^x \cos y$, $f_2(x,y) = e^x \sin y$. Show that the Jacobian of f is not zero at any point of $\mathbb{R}^2$.

Unit II

V (a) Prove that the outer measure of an interval is its length.

(b) Let $\{f_n\}$ be a sequence of measurable functions with the same domain of definition. Prove that $\sup_n f_n$ and $\inf_n f_n$ are measurable functions.

VI (a) Prove that there exists a nonmeasurable set.

(b) Let $\{f_n\}$ be an increasing sequence of nonnegative measurable functions and let $f = \lim f_n$ *a.e.*. Prove that $\int f = \lim \int f_n$.

VII (a) Prove that the collection $\mathcal{M}$ of all Lebesgue measurable sets is a σ-algebra.

(b) Let f be a bounded function defined on $[a, b]$. If f is Riemann integrable on $[a, b]$, then prove that f is measurable and

$$R\int_a^b f\,dx = \int_a^b f\,dx.$$

Unit III

VIII (a) Let f and g be integrable over a measurable set E. Prove that $f + g$ is integrable over E and

$$\int_E f + g = \int_E f + \int_E g.$$

(b) Let $\{f_n\}$ be a sequence of measurable functions that converges in measure to f. Prove that there exists a subsequence $\{f_{n_k}\}$ which conveges to f almost everywhere.

IX (a) Let f be a function defined as follows:

$$f(x) = \begin{cases} x\sin(\frac{1}{x}) & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}.$$

Find D^+f, D_+f, D^-f and D_-f at $x = 0$.

(b) Let f be an increasing real valued function on the interval $[a, b]$. Prove that f is differentiable almost everywhere. Also prove that the derivative f' is measurable and

$$\int_a^b f'(x)\,dx \leq f(b) - f(a).$$

X (a) Let f be an integrable function on $[a, b]$ and let

$$F(x) = F(a) + \int_a^x f(t)\,dt.$$

Prove that $F'(x) = f(x)$ for almost all x in $[a, b]$.

(b) If f is absolutely continuous, then prove that f has a derivative almost everywhere.

C 56858 (Pages : 3) Name..................................

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

SECOND SEMESTER M.Sc. DEGREE EXAMINATION, JULY 2009

Mathematics

Paper X—NUMBER THEORY

(2003 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

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

1. (a) Prove that for any integer $n \geq z$ $\varphi(n) \geq \frac{n}{2}$.

   (b) Find all x which simultaneously satisfy the system of congruencies.

   $x \equiv z \pmod 4$, $x \equiv 5 \pmod 7$, $x \equiv 9 \pmod{11}$.

   (c) Let p be an odd prime. Prove that every reduced residue system mod p contains exactly $(p-1)/2$ quadratic residues.

   (d) Find the inverse of :

   $$A = \begin{pmatrix} 2 & 3 \\ 7 & 6 \end{pmatrix} \in \mu_2 \left(\mathbb{Z}/26\,\mathbb{Z} \right).$$

(4 × 4 = 16 marks)

Part B

Answer any **four** *questions without omitting any unit.*
Each question carries 16 *marks.*

UNIT I

2. (a) Prove that :

   (i) $\varphi(mn) = \varphi(m)\varphi(n) \big/ \varphi((m,n))$.

   (ii) a/b suplier $\varphi(a) \big/ \varphi(b)$.

   (b) Suppose that g and $f * g$ are multiplicative Arithematics functions, prove that f is also multiplicative.

Turn over

3. (a) Prove that for all $x \geq 2$.

$$\left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| < 1.$$

(b) Assume that f is a multiplicative function. Prove that f is completely multiplicative of and only if $f^{-1}(p^n) = 0$ for all prime p and all integers $n \geq 2$.

4. (a) Prove that for $n \geq 1$, the n^{th} prime p_n satisfies the equalities

$$\frac{1}{6} n \log n < p_n < 12 \left(n \log n + n \log \frac{12}{e} \right).$$

(b) State Shapiro's Tauberian theorem.

Unit II

5. (a) State and prove that Chinese remainder theorem.

(b) For any prime $p \geq 5$, prove that $\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p^2}$.

6. (a) For every add prime p, prove that $\left(2/p \right) = (-1)^{(p^2-1)/8}$.

(b) State and prove the principle of cross classification.

7. (a) State and prove Gauss Lemma.

(b) Let p be a prime $\equiv 3 \pmod 4$ Prove that

$$\sum_{r=1}^{p-1} (r/p) = p \sum_{r=1}^{p-1} r\,(r/p).$$

Unit III

8. (a) Describe encryption using encephering matrices.

Illustrate with an example.

(b) Solve the system of simultaneous linear congruence.

$x + 3y \equiv 1 \pmod{26}$

$7x + 9y \equiv 1 \pmod{26}$

9. (a) Explain the ideas behind public key Cryptography and how it is used in conjunction with classical crypto systems (key exchange)

(b) Explain the importance and methods of authentication in public key crypto system.

10. (a) Explain the precautions to be taken in choosing the two prime band q in the RSA crypto system.

(b) Find the discrete log of 7 to the base 2 in F^*_{37} using the silver Pohliz-Hellman algorithm.

(4 × 16 = 64 marks)

C 56857 (3 Pages) Name..................................

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

SECOND SEMESTER M.Sc. DEGREE EXAMINATION, JUNE 2009

Mathematics

Paper IX—PARTIAL DIFFERENTIAL EQUATIONS AND INTEGRAL EQUATIONS

(2003 Admissions)

Time : Three Hours Maximum : 80 Marks

Answer **all** *questions from Part A and any* **four** *questions from Part B without omitting any unit.*

Part A

Each question carries **4** *marks.*

1. Find the general integral of $y^2 p - xyq = x(z - 2y)$.

2. Solve the initial value problem for the quasi-linear equation $zz_x + z_y = 1$ with the initial conditions $x = s, y = s, z = \frac{1}{2} \cdot s$ for $0 \le s \le 1$.

3. Suppose that $u(x, y)$ is harmonic in a bounded domain D and continuous in $\overline{D} = D \cup B$. Show that u attains its minimum on the boundary B of D.

4. Determine the iterated kernel $k_2(x, \xi)$ associated with $k(x, \xi) = |x - \xi|$ in$(0,1)$.

(4 × 4 = 16 marks)

Part B

Each question carries **16** *marks.*

Unit I

I. (a) Show that a necessary and sufficient condition that the p faffian differential equation $\vec{X} \cdot \vec{dr} = P(x, y, z)\,dx + Q(x, y, z)\,dy + R(x, y, z)d_z = 0$, be integrable is that $\vec{X} \cdot \text{curl}\,\vec{X} = 0$.

(b) Find the integral of $yz\,dx + 2xz\,dy - 3xydz = 0$.

II. (a) Show that the equations $p^2 + q^2 - 1 = 0$, $(p^2 = q^2)\,x - pz = 0$ are compatible and find the one-parameter family of common solutions.

(b) Solve the equation $z^3 = pq\,xy$ by Jacobi's method.

Turn over

III. (a) Find a solution of $(p^2 + q^2)\, x = pz$ passing through the parabola $x = 0,\ z^2 = 4y$.

(b) Find the characteristic strips of the equation $xp + yq - pq = 0$ and obtain the equation of the integral surface through the curve $C = z = x/2,\ y = 0$.

Unit II

IV. (a) Reduce the equation $x^2\, u_{xx} - y^2\, u_{yy} = 0$ into canonical form.

(b) Obtain the solution which describes the vibrations of a semi-infinite string.

V. (a) Solve :

$$\begin{aligned} &y_{tt} - c^2\, y_{xx} = 0,\ 0 < x < 1,\ t > 0 \\ &y\,(0, t) = y\,(1, t) = 0, \\ &y\,(x, 0) = x\,(1 - x),\ 0 \le x \le 1 \\ &y_t\,(x, 0) = 0,\ 0 \le x \le 1. \end{aligned}$$

(b) Show that the solution of the following problem, if it exists, is unique.

$$\begin{aligned} &u_{tt} - c^2\, u_{xx} = F\,(x, t),\ 0 < x < l,\ t > 0 \\ &u\,(x, 0) = f(x),\ 0 \le x \le l, \\ &u_t\,(x, 0) = g\,(x),\ 0 \le x \le l, \\ &u\,(0, t) = u,\,(l, t) = 0,\ t \ge 0. \end{aligned}$$

VI. (a) Solve the Dirichlet problem for a half plane.

(b) Discuss the heat conduction problem in an infinite rod.

Unit III

VII. (a) Transform the problem $\dfrac{d^2y}{dx^2} + y = x,\ y\,(0) = 1,\ y'\,(1) = 0$ to a Fredhom integral equation.

(b) Show that the Green's function for the Bessel operator or order n, $Zy - \dfrac{d}{dx}\left(x\,\dfrac{dy}{dx}\right) - \dfrac{n^2}{x}\, y$, relevant to the end conditions $y(0) = y(1) = 0$, is of the form

$$G\,(x, \xi) = \begin{cases} \dfrac{x^n/\xi^n}{2_n}\,(1 - \xi^{2n}) \text{ when } x < \xi, \\[2ex] \dfrac{\xi^n/x^n}{2_n}\,(1 - x^{2n}) \text{ when } x > \xi, \end{cases}$$

when $n \neq 0$.

VIII. (a) Show that any solution of the equation $y(x) = \lambda \int_0^1 (1 - 3x\xi)\, y(\xi)\, d\xi + F(x)$ can be expressed as the sum of F (x) and some linear combination of the characteristic functions.

(b) Show that the characteristic values of λ for the equation $\lambda \int_0^{2\pi} \sin(x+\xi)\, y(\xi)\, d\xi$ are $\lambda_1 = 1/\pi$ and $\lambda_2 = -1/\pi$, with corresponding characteristic functions of the form $y_1(x) = \sin x + \cos x$ and $y_2(x) = \sin x - \cos x$.

IX. (a) Describe the method of successive approximation of solving certain integral equation the second kind.

(b) Apply the method in part (*a*) to solve the equation $y(x) = \int_0^x (x+\xi)\, y(\xi)\, d\xi + 1$ taking $y^0(x) = 1$.

(4 × 16 = 64 marks)

56856

(Pages : 2)

Name.....................................

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

SECOND SEMESTER M.Sc. DEGREE EXAMINATION, JUNE 2009

Mathematics

Paper VIII—TOPOLOGY—I

(2003 Admissions)

Time : Three Hours | Maximum : 80 Marks

Part A

Answer **all** *the questions.*
Each part carries 4 *marks.*

I. (a) Is the open interval (0, 1) in R with usual topology compact ? Justify your claim.

(b) Give an example of a topological space that is T_2 but not T_3.

(c) Prove that every quotient space of a discrete space is discrete.

(d) Give an example of a continuous function on the set of real numbers with usual topology.

(4 × 4 = 16 marks)

Part B

Answer any **four** *questions without omitting any unit.*
Each question carries 16 *marks.*

UNIT I

II. (a) Prove that a set is closed with respect to a topology if and only its complement is open.

(b) Give an example of topology on the set of real numbers that is stronger than the usual topology.

III. (a) Exhibit all the topological spaces on the set $X = \{a, b, c\}$.

(b) Prove that second countability is a hereditary property.

IV. (a) Obtain the closure of the set of rational numbers in the set of real numbers with usual topology.

(b) Define derived set of a set in a topological space. Find the derived set of the open interval (0, 1) in the set of real numbers with usual topology.

UNIT II

V. (a) Define product topology. Prove that product topology is the weak topology determined by the projection functions.

(b) Give an example of a quotient map in the set of real numbers with usual topology.

VI. (a) Write an example of a space that is separable and prove your claim.

(b) Prove that every continuous image of a compact space is compact.

Turn over

VII. (a) Prove that a subset of R with usual topology is connected if and only it is an interval.

(b) Let $f : X \rightarrow Y$ be a function where X and Y are topological spaces and Y have the quotient topology on it with respect to f. Then for any topological space Z, prove that a function $g : Y \rightarrow Z$ is continuous if and only if $g \circ f : X \rightarrow Z$ is continuous.

UNIT III

VIII. (a) Give any *two* definitions of a T_1 space and prove their equivalence.

(b) Define regular space. Prove that every completely regular space is regular.

IX. (a) Prove that a metric space is a T_4 space.

(b) Prove that every compact Hausdorff space is a normal space.

X. (a) State and prove Urysohn's lemma.

(b) Prove that regularity is a hereditary property in topological spaces.

(4 × 16 = 64 marks)

C 56855 (Pages : 2)

Name....................................

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

SECOND SEMESTER M.Sc. DEGREE EXAMINATION, JULY 2009

Mathematics

Paper VII—REAL ANALYSIS—II

(2003 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

Answer **all** *the questions.*
Each part carries 4 *marks.*

I. (a) Give an example of linear operator A on R^n that is one-to-one. Without actual verification, prove that the range of A is all of R_n.

(b) Given any collection C of subsets of X, prove that there is a smallest algebra A which contains C.

(c) Let f be a nonnegative measurable function. Show that $\int f = 0$ implies $f = 0$ a.e.

(d) If f and g are integrable function over E, then prove that $f + g$ is also integrable over E.

Part B

Answer any **four** *questions without omitting any unit.*
Each question carries 16 *marks.*

Unit I

II. (a) If Ω is the set of all invertible linear operators on R^n, then prove that Ω is an open subset of L (R^n) and the mapping $A \to A^{-1}$ is continuous on Ω.

(b) State and prove the inverse function theorem.

III. (a) Suppose f maps an open set $E \subset R^n$ into R^m. Then prove that f is continuously differentiable in E if and only if the partial derivatives $D_j f_i$ exist and are continuous on E for $1 \leq i \leq m$ and $1 \leq j \leq n$.

(b) If the matrix $[A]_1$ is obtained from the matrix [A] by interchanging two columns, then that det $[A]_1 = -$ det [A].

IV. (a) Define a contraction function. Give an example. Prove that if X is a metric space and ϕ is a contraction of X into X, then there exist one and only one $x \in X$ such that $\phi(x) = x$.

(b) State and prove the implicit function theorem.

Turn over

Unit II

V. (a) Prove that the outer measure of an interval is its length.

(b) Define Lebesgue measurable function. If f is Lebesgue measurable and $f = g$ a e., then prove that g is Lebesgue measurable.

VI. (a) Define measurable set. Prove that the family of measurable sets is an algebra of sets.

(b) Define Riemann upper integral and lower integral of a function. Give an example of a function where the lower and upper integrals are different.

VII. (a) State and prove the Bounded Convergence theorem.

(b) Let u_n be a sequence of non-negative measurable functions and let $f = \sum_{n=1}^{\infty} u_n$. Then prove that

$$\int f = \sum_{n=1}^{\infty} \int u_n .$$

Unit III

VIII. (a) State and prove the Lebesgue Convergence theorem.

(b) Let $\langle f_n \rangle$ be a sequence of measurable functions that converges in measure to f. Then prove that there is subsequence $\langle f_{nk} \rangle$ that converges to f almost everywhere.

IX. (a) Define function of bounded variation. If f is integrable on $[a,b]$, then prove that the function F defined by

$$F(x) = \int_a^x f(t)\,dt$$

is a continuous function of bounded variation on $[a, b]$.

(b) Define absolute continuity of a real valued function. If f is a absolutely continuous on $[a, b]$, then prove that it is of bounded variation on $[a, b]$.

X. (a) Prove that a function f is of bounded variation on $[a, b]$, if and only if f is the difference of two monotone real-valued functions on $[a, b]$.

(b) Construct a monotone function on [0,1] which is discontinuous at each rational point.

C 48238 (Pages : 2)

Name..................................

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

SECOND SEMESTER M.Sc. DEGREE EXAMINATION, AUGUST 2008

Mathematics

Paper X—NUMBER THEORY

(2003 admissions)

Time : Three Hours | Maximum : 80 Marks

Part A

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

1. (a) Find all integers n such that Q (n) = Q$(2n)$.

   (b) Prove that $\prod_{t/n} t = n^{d(n)/2}$ where $d(n)$ denotes the number of positive densors of n.

   (c) For an odd prime p, prove that $(-1\,|\,p) = (-1)^{(p-1)/2}$.

   (d) Find the inverse of the matrix $\begin{pmatrix} 40 & 0 \\ 0 & 1 \end{pmatrix}$ and 841.

(4 × 4 = 16 marks)

Part B

Answer any **four** *questions without omitting any unit.*
Each question carries 16 *marks.*

UNIT I

2. (a) For $n > 1$, prove that Q $(n) = n \prod_{p/n} (1 - 1/p)$.

   (b) State and prove the Möbius inversion formula.

3. (a) State and prove Euler's summation formula.

   (b) Prove that $\sum_{n \le x} \frac{1}{n} = \log x + c + 0\left(\frac{1}{x}\right)$, where c denotes Euler's constant.

4. (a) State and prove Abel's identify.

   (b) Prove that the relation $\lim_{x \to \infty} \frac{\pi(x) \log x}{x} = 1$ is logically equivalent to the relation $\lim_{x \to \infty} \frac{\theta(x)}{x} = 1$.

Turn over

Unit II

5. (a) Suppose that a and m are relatively prime integers. Prove that the congruence :

$$ax \equiv b \pmod{m}$$

has a unique solution.

(b) Prove that the set of lattice points in the plane visible from the origin contains arbitrarily large square gaps.

6. (a) Prove that the Legendre symbol (x/p) is a completely multiplicative function of n.

(b) Prove that $(2/p) = (-1)^{(p^2-1)/8}$, where p is an odd prime.

7. (a) State and prove Gauss lemma.

(b) Let p be an odd prime. Prove that $\sum_{n=1}^{p-1} r(r/p) = 0$ if $p \equiv 1 \bmod 4$.

Unit III

8. (a) Explain the terms cryptosystem and cryptanalysis. Illustrate with example.

(b) Working in the 26 letter alphabet A – Z (with corresponding numbers 0 – 25 encipher the message "PAY ME NOW" using the affirm transformation with key $a = 7$; $b = 12$.

9. (a) Suppose, it is known that the adversary is using an enciphering matrix A in the 26 letter alphabet. The cipher text "WKNCCHSSJH" is intercepted and it is known that the first word is "GIVE".

Find the deciphering matrix A^{-1} and read the message.

(b) Explain the principles underlying public key cryptosystem.

10. (a) Write short notes on :

(i) RSA cryptosystem.

(ii) Diffie-Hellman key exchange system.

(b) Find the discrete log of 28 to the base 2 in F_{37}^{*} using the silver Pohlig-Hellman algorithm, 2 being a generator of F_{37}^{*}.

(4 × 16 = 64 marks)

C 48237 (Pages : 3) Name..................................

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

SECOND SEMESTER M.Sc. DEGREE EXAMINATION, AUGUST 2008

Mathematics

Paper IX—PARTIAL DIFFERENTIAL EQUATIONS AND INTEGRAL EQUATIONS

(2003 Admissions)

Time : Three Hours Maximum : 80 Marks

Part A

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

1 Form the partial differential equation by eliminating the arbitrary function F from the equation $F\left(x+y, x-\sqrt{z}\right)=0$.

2. Find the complete integral of the equation $zpq-p-q=0$.

3. Show that the solution to the Dirichlet problem to the Laplace's equation in stable.

4. Explain the terms Fredhom equation, Kernel of the integral equation and the volterra equation.

(4 × 4 = 16 marks)

Part B

Answer any **four** *questions without omitting any unit.*
Each question carries 16 marks.

UNIT I

I. (a) Show that the general solution of the quasi-linear equation :

$$P(x, y, z)\, p + Q(x, y, z)\, q = R(x, y, z)$$

where P, Q, R are given continuously differentiable functions of x, y and z is $F(u, v) = 0$, where F is an arbitrary function of u and v and $u(x, y, z) = C_1$ and $v(x, y, z) = C_2$ are the solutions, of the system $\dfrac{dx}{P(x,y,z)} = \dfrac{dy}{Q(x,y,z)} = \dfrac{dz}{R(x,y,z)}$.

(b) Find the general integral of $(y+1)\,p + (x+1)\,q = z$.

II. (a) Obtain a necessary and sufficient condition for the compatibility of the equation $f(x, y, z, p, q) = 0$ and $g(x, y, z, p, q) = 0$.

(b) Show that the equations $p^2 + q^2 - 1 = 0$ and $(p^2 + q^2)\,x - pz = 0$ are compatible and find the one-parameter family of common solutions.

Turn over

III. (a) Find the complete integral of the equation $p^2x + qy - z = 0$ and derive the equation of the integral surface containing the line $y = 1, x + z = 0$.

(b) Solve the Canchy problem for $2z_x + yz_y = z$, when the initial data curve is C : $x_0 = S, y_0 = s^2, z_0 = s, 1 \leq s \leq 2$.

UNIT II

IV. (a) Reduce the equation $4u_{xx} - 4u_{xy} + 5u_{yy} = 0$ into its canonical form.

(b) Solve the equation :

$$(n-1)^2 u_{xx} - y^{2n} u_{yy} = ny^{2n-1} u_y$$

by reducing it into canonical form.

V. (a) Show that :

$$v(x,y\,;\alpha,\beta) = \frac{(x+y)\left[2xy + (\alpha-\beta)(x-y) + 2\alpha\beta\right]}{(\alpha+\beta)^3}$$

is the Riemann function for the second order partial differential equation

$$u_{xy} + \frac{2}{x+y}\left(u_x + u_y\right) = 0.$$

(b) Solve : $y_{tt} - C^2 y_{xx} = 0, 0 < x < 1, t > 0,$

$$y(0, t) = y(1, t) = 0,$$

$$y(x, 0) = 0, 0 \leq x \leq 1$$

$$y_t(x, 0) = x^2, 0 \leq x \leq 1$$

VI. (a) Obtain Green's function for Laplace's equation.

(b) Solve Dirichlet problem for a circle.

UNIT III

VII. (a) If $y''(x) = F(x)$, and y satisfies the end conditions $y(0) = 0$, and $y(1) = 0$, show that $y(x) = \int_0^1 k(x,\xi)\,F(\xi)\,d\xi$, where K (x, ξ) is defined by the relations $K(x,\xi) = \begin{cases} \xi(x-1) & \text{when } \xi < x \\ x(\xi-1) & \text{when } \xi > x \end{cases}$.

(b) Show that, if $y(x)$ satisfies the differential equation $\frac{d^2y}{dx^2} + xy = 1$ and the conditions $y(0) = y'(0) = 0$, then y also satisfies the volterra equation $y(x) = \int_0^x \xi(\xi - x)\,y(\xi)\,d\xi + \frac{1}{2}x^2$.

VIII (a) Determine $p(x)$ and $q(x)$ in such a way that the equation :

$$x^2 \frac{d^2y}{dx^2} - 2x\frac{dy}{dx} + 2y = 0.$$

is equivalent to the equation $\frac{d}{dx}\left(p\frac{dy}{dx}\right) + qy = 0$, thus showing that the equation can be written in the self-adjoint form $\frac{1}{dx}\left(\frac{1}{x^2}\frac{dy}{dx}\right) + \frac{2}{x^4}y = 0$.

(b) Verify that $u(x) = x$ and $v(x) = x^2$ are linearly independent solutions of the equation of part (*a*).

IX. (a) Describe the method of successive approximation of solving certain integral equation of the second kind.

(b) Solve by the method of successive approximation :

$$y(x) = 1 + \lambda \int_0^1 (1 - 3x\xi)\, y(\xi)\, d\xi.$$

(4 × 16 = 64 marks)

C 48236 (Pages : 2)

Name..................................

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

SECOND SEMESTER M.Sc. DEGREE EXAMINATION, AUGUST 2008

Mathematics

Paper VIII—TOPOLOGY—I

(2003 Admissions)

Time : Three Hours

Maximum : 80 Marks

Part A

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

I. (a) Define diameter of a set in a matric space. Let (X, d) be a metric space and $A = \{(x, y) : 1 < d(x, y) < 2 ; x, y \in X\}$, find the diameter of A.

(b) Give an example of a continuous function in the set of real numbers with usual topology.

(c) Prove that a metric space is a T_4 space.

(d) Prove that the unit circle in R^2 with usual topology is compact.

($4 \times 4 = 16$ marks)

Part B

Answer any **four** *questions without omitting any unit.*
Each question carries 16 *marks.*

Unit I

II. (a) Define open set in a topological space. In the set of real numbers with usual topology, give an example of an open set and justify the claim.

(b) Define the semi-open interval topology on the set of real numbers. Prove that this topology is stronger than the usual topology.

III. (a) Define second countable space. Prove that in a second countable space, every open cover of it has a countable sub-cover.

(b) Prove that second countability is a hereditary property.

IV. (a) Define derived set and closure of a set in a topological space. Obtain the relation connecting a set, its closure and the derived set.

(b) Find the derived set of the open interval (0, 1) in the set of real numbers with usual topology.

Unit II

V. (a) Define product topology. Prove that product topology is the weak topology determined by the projection functions.

(b) Define quotient map. Prove that every open surjective map is a quotient map.

Turn over

VI. (a) Define divisible topological property. Prove that the property of being a discrete space is divisible.

(b) Define separable space. Give an example of a space that is separable and prove your claim.

VII. (a) Prove that every continuous real-valued function on a compact space is bounded and attains its extrema.

(b) Prove that a subset of R with usual topology is connected if and only it is an interval.

UNIT III

VIII. (a) Give an example of a topology on a set X that is T_1 but not T_2.

(b) Define regular space. Prove that every completely regular space is regular.

IX. (a) Give an example to show that a regular space need not be completely regular.

(b) Prove that every compact Hausdorff space is a T_3 space.

X. (a) State and prove Urysohn's lemma.

(b) Give an example of a set in R^2 with usual topology that is not compact and justify the claim.

(4 × 16 = 64 marks

C 48234 (Pages : 2) Name..................................

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

SECOND SEMESTER M.Sc. DEGREE EXAMINATION, AUGUST 2008

Mathematics

Paper VI—ALGEBRA—II

(2003 admissions)

Time : Three Hours Maximum : 80 Marks

Answer **all** *questions in Part A.*
Each question carries 4 marks.
Answer any **four** *questions in Part B without omitting any unit.*
Each question carries 16 marks.

Part A

I. (a) Verify whether every quotient of an integral domain is again an integral domain.

(b) Let α be the real cube root of 2. Verify whether $Q(\alpha)$ is a splitting field over CD.

(c) Find all automorphisms of $\left(i, \sqrt{2}\right)$.

(d) Describe the Galois group of the polynomial x^3 - . over Q.

(4 × 4 = 16 marks)

. : 3

UNIT .

II. (a) ... of a field.

... a field. Prove that :

(i) if F is of prime characteristic th. F contains a subfield isomorphic to Z_p.

(ii) if F is of characteristic zero, then F contains a subfield isomorphic to the field Q of rationals.

III. (a) Let F be a field and α be algebraic over F. Let deg irr (α ; F = n. Show that every $\beta \in F(\alpha)$ can be uniquely expressed as $\beta = b_0 + b_1 \alpha + \ldots + b_{n-1} \alpha^{n-1}$, where $b_i \in$ F.

... $\sqrt{1+\sqrt{3}}$, find irr (α, Q), where Q is the field of rationals.

... (a) Prove that if α and β are constructible real numbers, then $\alpha\beta$ is constructible.

(b) Prove the impossibility of trisecting an angle using straight edge and compass.

Turn over

UNIT 2

V. (a) Show that a finite field of p^n elements exists for every prime p and every positive integer n.

(b) If F is a finite field and n is a positive integer, prove that an irreducible polynomial of degree n exists in F[x].

VI. (a) Let F be a field and $\overline{F}$ be an algebraic closure of F. Let $\alpha \in \overline{F}$ and $\psi : F(\alpha) \to \overline{F}$ be an isomorphism with $\psi(a) = a$ for every $a \in F$. Prove that α and $\psi(\alpha)$ are conjugates over F.

(b) Find all isomorphisms of $Q(\sqrt{3})$ into $\bar{Q}$, where $\bar{Q}$ is the algebraic closure of Q.

VII. (a) Define splitting field. Let $\overline{F}$ be an algebraic closure of F and $F \leq E \leq \overline{F}$. Show that if E is a splitting field over F then every automorphism of $\overline{F}$ leaving F fixed, maps E onto E.

(b) Show that if E is a splitting field over F of finite degree then $\{E : F\} = |G(E/F)|$.

UNIT 3

VIII. Let K be a finite normal extension of a field F and $F \leq E \leq K$. Define $\lambda(E) = G(K/E)$ for every E with $F \leq E \leq K$. Prove that :

(i) the fixed field of G(K/E) in K is E

(ii) λ is one-to-one.

(iii) $[K : E] = |\lambda(E)|$.

IX. (a) Define cyclotomic extension. Prove that the Galois group of the n^{th} cyclotomic extension of the field Q of rationals has $\varphi(n)$ elements where φ is the Euler phi-function.

(b) Prove that the Galois group of the p^{th} cyclotomic extension of Q where p is a prime is isomorphic to the cyclic group of order $p - 1$.

X. (a) Define solvable group. State a theorem relating solvability by radicals and solvable groups.

(b) Establish the insolvability of the quintic.

($4 \times 16 = 64$ marks)

C 7234 (Pages : 2)

Name..

Reg. No..

SECOND SEMESTER M.Sc. DEGREE EXAMINATION, AUGUST 2005

Mathematics

Paper VIII—TOPOLOGY—I

(2003 admissions)

Time : Three Hours Maximum : 80 Marks

Part A

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

I. (a) Let (X, d) be a metric space and A be a subset of X defined by :

$$A = \{(x, y) : 1 < d(x, y) \leq 2 ; x, y \in X\}.$$

Calculate the diameter of the set A.

(b) Give an example for a topological space which is separable but not second countable.

(c) Define a Tychonoff space and give an example.

(d) Prove that a topological space is T_1 if and only if every singleton set is closed.

(4 × 4 = 16 marks)

Part B

Answer any **four** *questions without omitting any unit.*
Each question carries 16 *marks.*

UNIT I

II. (a) Prove that the function $f(x) = (\cos(\pi/2)x, \sin(\pi/2)x)$ establishes a homeomorphism between the unit interval [0, 1] in the set of real numbers with usual topology to the first quadrant arc of the unit circle in the two dimensional plane with usual topology.

(b) Define the semi-open interval topology on the set of real numbers. Prove that this topology is stronger than usual topology.

III. (a) Let $Z \subset Y \subset X$ and T be a topology on X. Then prove that

$$(T / Y)/Z = T / Z$$

where T / Y denotes the subspace topology on Y induced by T.

(b) Prove that the set of rationals is a dense subset of the set of real numbers under the usual topology.

IV. (a) Let X and Y be two topological spaces. Give an example of a continuous function from X to Y.

(b) Find the derived set of the open interval (0, 1) in the set of real numbers with usual topology.

Turn over

Unit II

V. (a) Define quotient map. Prove that every open, surjective map is a quotient map.

(b) Prove that every quotient space of a discrete space is discrete.

VI. (a) Prove that every continuous image of a compact space is compact.

(b) Prove that the real line with usual topology is not compact. Give a topology on the real line so that the resulting space is compact.

VII. (a) Define weakly hereditary property in a topological space. Give an example of a property that is weakly hereditary.

(b) Prove that a subset of R, the set of real numbers with usual topology, is connected if and only if it is an interval.

Unit III

VIII. (a) Give an example of a topology on a set X that is T_1 but not T_2.

(b) Prove that all metric spaces are T_4.

IX. (a) Prove that a compact subset of a Hausdorff space is closed.

(b) Define regular topological spaces. Prove that regularity is a hereditary property.

X. (a) Prove that the unit circle in R^2 with usual topology is compact.

(b) State Urysohn's lemma. Using the lemma, prove that all T_4 spaces are completely regular.

(4 × 16 = 64 marks)

C 7031

(2 Pages)

Name ....

Reg. No ....

SECOND SEMESTER M.Sc. DEGREE EXAMINATION, AUGUST 2005

Mathematics

Paper X—NUMBER THEORY

(2001 admissions)

Time : Three Hours

Maximum : 80 Marks

Part A

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

1. (a) Prove that $\prod_{t/n} t = n^{d(n)/2}$.

 (b) For $x > 0$, prove that $\psi(x) = \sum_{m \le \log_2 x} \theta\left(x^{1/m}\right)$.

 (c) Prove that $5n^3 + 7n^5 \equiv 0 \pmod{12}$ for all integers n.

 (d) For the sequence (2, 3, 7, 20, 35, 69) and "volume" V = 45, determine whether the Knapsack problem is super increasing and how many solutions it has.

(4 × 4 = 16 marks)

Part B

Answer any **four** *questions without omitting any unit.*
Each question carries 16 *marks.*

UNIT I

2. (a) Prove that $\sum_{d/n} \mu(d) = \left[\frac{1}{n}\right]$ for $n \ge 1$.

 (b) Prove that formula : $\varphi(mn) = \varphi(m).\ \varphi(n)/\varphi(d)$, where $d = (m, n)$.

 (c) State and prove that the Möbius inversion formula.

3. (a) Prove that $\sum_{x>x} 1/n^s = 0\left(x^{1-s}\right)$, if $s > 1$.

 (b) Prove that $\pi(n) > \frac{1}{6}\, n/\log n$ for $n \ge 2$.

4. (a) State and prove Shapiro's Tauberian Theorem.

 (b) Assuming the prime number Theorem, prove that $\pi(8x)/\pi(2x) \sim 4$ as $x \to \infty$.

Turn over

UNIT II

5. (a) State and prove the Euler–Fermat theorem.

(b) Prove that the set of lattice points visible from the origin contains arbitrarily large square gaps.

6. (a) Let p be an odd prime. Then prove that $(n/p) = n^{(p-1)/2} \pmod p$ for all n.

(b) Determine whether 888 is a quadratic residue or non-residue of the prime 1999.

7. (a) State and prove Gauss' Quadratic reciprocity law.

(b) Let h and k be positive integers with h odd, then prove that

$$G(h; k) = \sqrt{\frac{k}{h}}\ \frac{1+i}{2}\left(1+e^{-\pi i \frac{hK}{2}}\right)\overline{G(k; h)},$$

UNIT III

8. (a) Explain the construction of affaine cryptosystems with digraphs.

(b) Encipher the message unit "ON" using the enciphering matrix $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2\left(\mathbb{Z}/_{26}\mathbb{Z}\right)$.

9. (a) Explain the RSA cryptosystem and illustrate with an example.

(b) How do we send a signature in RSA cryptosystem ?

10. (a) Explain the silver–Pohlig–Hellman algorithm for computing discrete logarithms in finite fields.

(b) Explain the Merkle–Hellmann cryptosystem.