DEPARTMENT OF MATHEMATICS

MADRAS CHRISTIAN COLLEGE
(AUTONOMOUS)

M.Phil. Mathematics

Curriculum & Syllabi

(with effect from 2016 – 2017)

M.Phil. (Mathematics) Curriculum
with effect from 2016 – 17

S. No.	Course	Hours	Marks			Credits
			CA	ESE	TOTAL	
Semester I						
1	Algebra and Cryptography	4	50	50	100	5
2	Analysis and Geometric Function Theory	4	50	50	100	5
3	Theory of Computation and Graph Theory	4	50	50	100	5
	Total	**12**				**15**
Semester II						
4	Dissertation	12	50	50	100	21
	Total	**12**				**21**
	Grand Total					**36**

Algebra and Cryptography

Semester: I **Credits: 5**

Paper: 1 **Hours / Cycle: 4**

Unit I

Rings, Ideals, Homomorphism of rings.

Chapters: 1, 2, 3

Unit II

Modules, Modules with Chain Conditions

Chapter 5: Sections 5.1 – 5.8, Chapter 6

Content and treatment as in

Introduction to Rings and Modules, Second Revised Edition, C. Musili, Narosa Publishing House, New Delhi, 1994.

Unit III

An introduction to Cryptography, Discrete Logarithms and Diffie-Hellman.

Chapters 1, Chapter 2: Sections 2.1 – 2.4

Unit IV

Integer Factorization and RSA, Elliptic Curves and Cryptography.

Chapter 3: Sections 3.1 – 3.3, Chapter 5: Sections 5.1 – 5.4

Content and treatment as in

J. Hoffstein, J. Pipher and J.H. Silverman, An Introduction to Mathematical Cryptography, Springer (India) Pvt. Ltd., New Delhi, 2008.

References

1. M.F. Atiya and I.G. Macdonald, Commutative Algebra, Addison-Wesley, Great Britain, 1969.
2. S. Lang, Algebra, Addison-Wesley, USA, 1993.
3. M. Artin, Algebra, Pearson, New Delhi, 1991.
4. J.A. Buchmann, Introduction to Cryptography, Springer, New Delhi, 2001
5. N. Koblitz, Introduction to Number Theory and Cryptography, Springer, New Delhi, 1994.
6. D. Stinson, Cryptography, Theory and Practice, CRC Press, London, 2002.

Analysis and Geometric Function Theory

Semester: I **Credits: 5**

Paper: 2 **Hours / Cycle: 4**

Unit I

Fourier Transforms – Formal properties – The Inversion theorem – The Plancherel theorem – The Banach algebra of L^1.

Holomorphic Fourier Transforms – Introduction – Two theorems of Paley and Wiener - Quasi-analytic classes – The Denjoy-Carleman theorem.

Chapter 9, Chapter 19

Unit II

Conformal Mapping – Preservation of angles – Linear fractional transformations – Normal families – The Riemann mapping theorem – The class S - Continuity at the boundary – Conformal mapping of an annulus.

H^p-Spaces – Sub-harmonic functions – The spaces H^p and N - The theorem of F and M. Riesz – Factorization theorems.

Chapter 14: Sections 14.1 – 14.8, Chapter 17: Sections 17.1 – 17.19

Content and Treatment as in

Real and Complex Analysis, Walter Rudin, Third Edition, McGraw–Hill International editions, Singapore, 1987.

Unit III

Univalent functions – Area enclosed by a contour – The interior area theorem – Prawitz's lemma - A mean value theorem – Faber's functions – An equality of Golusin – Distortion theorem – Bieberbach's theorem – The Koebe-Bieberbach theorem – A covering theorem for convex funtions – General Distortion theorems – Koebe's distortion theorem for general regions – A test for Normal families.

Chapter 11: Sections 11.1.1 – 11.2.3

Unit IV

General Distortion theorems – Koebe's distortion theorem for general regions – A test for Normal families.

Estimates of coefficients: A theorem of Littlewood – Odd functions – Typically real functions – Starlike univalent functions – Relation between Convex and Starlike functions.

Chapter 11: Sections 11.2.4 – 11.3.5

Content and Treatment as in

Geometric function Theory, Volume 2, G. Sansone and J. Gerretsen, Wolters-Noordhoff Publishing Groningen, Netherlands, 1969.

References

1. Theory of H^p – Spaces, P.L. Duren, Academic Press, New York, 1970.
2. Real and Abstract Analysis, Volume II, E. Hewitt & K. Stromberg, Springer, New York, 1965.
3. Univalent functions, Peter L Duren, Springer, New York, 1983.
4. Univalent functions, Volume 2, A.W. Goodman, Mariner Publishing Company, Florida, 1983.

Theory of Computation and Graph Theory

Semester: I **Credits: 5**
Paper 3 **Hours / Cycle: 4**

Unit I

The Church-Turing Thesis: Turing Machines, Variants of Turing Machines, Algorithm.

Decidability: Decidable Languages, The Halting Problem.

Chapter 3: Sections 3.1 – 3.3, Chapter 4: Sections 4.1, 4.2

Unit II

Reducibility: Undecidable Problems from Language Theory, A Simple Undecidable Problem, Mapping Reducibility.

Time Complexity: Measuring Complexity, The Class P, The Class NP, NP-completeness, Additional NP-complete Problems.

Chapter 5: Sections 5.1 – 5.3

Chapter 7: Sections 7.1 – 7.5

Content and Treatment as in

Michael Sipser, Introduction to the Theory of Computation, Second Edition, Thomson Course Technology, Boston, 2006.

Unit III

Domination in Graphs, Bounds in terms of Order, Bounds in terms of Order, Degree and Packing, Bounds in terms of Order and Size, Bounds in terms of Degree, Diameter and Girth, Bounds in terms of Independence and Covering

Chapter 1: Sections 1.1 – 1.2, Chapter 2: Sections 2.1 – 2.5

Content and Treatment as in

T.W. Haynes, S. T. Hedetniemi and P. J. Slater, Fundamentals of Domination in Graphs, Marcel Dekker Inc., New York, 1998.

Unit IV

T-Colourings, L(2,1)-colourings, Radio Colourings, Hamiltonian Colourings, Domination and Colourings.

Chapter 14: Sections 14.1 – 14.5

Content and Treatment as in

G. Chartrand and P. Zhang, Chromatic Graph Theory, CRC Press, New York, 2009.

References

1. J.E. Hopcroft and J.D. Ullman, Introduction to Automata Theory, Languages, and Computation, Narosa Publishing House, New Delhi, 1989.
2. J.E. Hopcroft, R. Motwani and J.D. Ullman, Introduction to Automata Theory, Languages, and Computation, Third Edition, Pearson Education, New Delhi, 2008.
3. R. Diestel, Graph Theory, Third Edition, Springer, Berlin, 2006.
4. D.B. West, Introduction to Graph Theory, PHI Learning Private Ltd., New Delhi, 2001.
5. J. Clark and D.A. Holton, A First Look at Graph Theory, Allied Publishers, New Delhi, 1995.

DEPARTMENT OF MATHEMATICS

MADRAS CHRISTIAN COLLEGE

(AUTONOMOUS)

M.Phil. Mathematics

Model Question Papers

(with effect from 2016 – 2017)

MADRAS CHRISTIAN COLLEGE (Autonomous)

DEPARTMENT OF MATHEMATICS

MODEL QUESTION PAPER

PAPER I - ALGEBRA AND CRYPTOGRAPHY

M.Phil. (i) **Time 3 Hours** **Max. Marks 100**

Answer any FIVE questions choosing at least TWO questions from each section. Each question carries TWENTY marks.

SECTION A

1. (a) Define a division ring. Give an example of a division ring which is not a field. (4)

   (b) If R is a ring with 1 and I is a left ideal in R such that $I \neq R$ then prove that there is a maximal left ideal M such that $I \subseteq M$. (8)

   (c) Let R be a commutative ring. Prove that a nil ideal I is nilpotent if I is finitely generated. (8)

2. (a) Prove that a homomorphism $f: R \to S$ is a monomorphism if and only if $Ker(f) = (0)$. (4)

   (b) State and prove epimorphism theorem. (8)

   (c) Let R be a commutative integral domain with 1. Define the set of fractions $Q(R)$ and prove that it is a field containing R as a subring. (8)

3. (a) When do we say that a module is finitely generated? Prove that any vector space is a free module. (6)

   (b) State and prove Schur's lemma. (6)

   (c) Prove the equivalence of descending chain condition and minimum condition for submodules of a module. (8)

4. (a) State and prove Jordan-Holder Theorem. (10)

   (b) State and prove Hilbert Basis Theorem. (10)

SECTION B

5. (a) Explain symmetric and asymmetric ciphers. Give an example for symmetric cipher. (10)

   (b) Write down the fast powering algorithm. Explain it with an example. (10)

6. (a) Define discrete logarithm problem. Explain Diffie – Hellman Key exchange algorithm. (10)

   (b) Discuss the difficulty of the discrete logarithm problem. (10)

7. (a) Explain RSA public key cryptosystem with an example. (10)

   (b) Solve the congruences:

   (i) $x^{1583} \equiv 4714 (mod 7919)$

   (ii) $x^{17389} \equiv 43927 (mod 64349)$ (5+5)

8. (a) Define an elliptic curve over a finite field. Explain the elliptic curve discrete logarithm problem. (10)

   (b) Explain Elliptic ElGamal public key cryptosystem. (10)

MADRAS CHRISTIAN COLLEGE (Autonomous)

DEPARTMENT OF MATHEMATICS

MODEL QUESTION PAPER

PAPER II – ANALYSIS AND GEOMETRIC FUNCTION THEORY

M.Phil. (i) **Time 3 Hours** **Max. Marks 100**

Answer any FIVE questions choosing at least TWO questions from each section. Each question carries TWENTY marks.

SECTION A

1. (a) State and prove Interior Area Thorem.

   (b) State and prove Prawitz Lemma

2. (a) State and prove Golusin inequality

   (b) State and prove Koebe's one fourth Theorem.

3. (a) State and prove Koebe Distortion Theorem.

   (b) State and prove Bieberbach rotation Theorem.

4. (a) State and prove Littlewood and Payley Theorem.

   (b) $f(z) = z + a_2z^2 + a_3z^3 + \cdots$ is typically real then prove that $|a_n| \leq n, n = 2,3,4, \ldots$

SECTION B

5. (a) State and prove Plancheral Theorem.

   (b) Show that $C(M_3)$ is an algebra with respect to pointwise multiplication.

6. State and prove Denjoy-Carleman Theorem.

7. (a) State $\subset H(\Omega)$and F is uniformly bounded on each compact subset of the region Ω then prove that F is a normal family.

   (b) Prove that $A\,(r_1, R_1)$ and $A\,(r_2, R_2)$ are conformally equivalent if and only if $\frac{R_1}{r_1} = \frac{R_2}{r_2}$

8. (a) Suppose that $f \in N, f \neq 0$ and B is the Blaschke product formed witht the zeros of f. Put $g = \frac{f}{B}$ then prove that $g \in N$ and $\|g_0\| = \|f_0\|$. Also prove that if $f \in H^p$ then $g \in H^p$ and $\|g\|_{\boldsymbol{p}} = \|f\|_{\boldsymbol{p}}$ $(0 < p \leq \infty)$.

   (b) If $(0 < p < \infty)$ and $f \in H^p$ then prove the following:

   (i) The non-tangential maximal functions $N_\alpha f$are in $L^p(T)$ for all $\alpha < 1$

   (ii) The non-tangential limits $f^*(e^{i\theta})$ exists a.e. on T and $f^* \in L^p(T)$

   (iii) $\lim_{r\to 1} \|f^* - f_r\|_{\boldsymbol{p}} = 0$ and

   (iv) $\|f^*\|_{\boldsymbol{p}} = \|f\|_{\boldsymbol{p}}$

MADRAS CHRISTIAN COLLEGE (Autonomous)

DEPARTMENT OF MATHEMATICS

MODEL QUESTION PAPER

PAPER III - THEORY OF COMPUTATION AND GRAPH THEORY

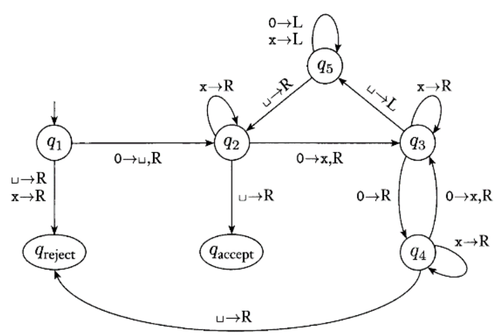
M.Phil. (i) **Time 3 Hours** **Max. Marks 100**

Answer any FIVE questions choosing at least TWO questions from each section. Each question carries TWENTY marks.

SECTION A

1. (a) Give the formal definition of a *Turing machine* (TM). Construct a TM that decides the language $\{(abc)^n / n \geq 1\}$. (10)

   (b) Find the language described by the TM having the following state diagram:



   Give the sequence of configurations the TM enters when started on the input 0000. (10)

2. (a) Define '*Turing decidable'*. Prove that E_{CFG} is decidable. (10)

   (b) What is a *'halting problem'*? Prove that 'halting problem' is undecidable. (10)

3. What is '*Post Correspondence Problem*' (PCP)? Prove that PCP is undecidable.

4. (a) Define '*Class P*' of languages. Prove that PATH € P. (10)

   (b) Describe '3-SAT problem'. Prove that 3-SAT is polynomial time reducible to CLIQUE problem. (10)

SECTION B

5. Show with the usual notation that a connected graph G satisfies $\gamma(G) = \lfloor n/2 \rfloor$ if and only if $G \in \mathcal{G} = \cup_{i=1}^{6} \mathcal{G}_i$.

6. a) If a graph G has $\delta(G) \geq 2$ and $g(G) \geq 5$, then prove that $\gamma(G) \leq \left\lceil \frac{n - \lfloor g(G)/3 \rfloor}{2} \right\rceil$. (10)

   b) For any graph G if $g(G) \geq 5$, then show that $\gamma(G) \geq \delta(G)$ and if $g(G) \geq 6$, then show that $\gamma(G) \geq (\delta(G) - 1)$. (10)

7. a) For every positive integer t, prove that $\lambda(K_{1,t}) = t + 1$. (10)

   b) If T is a tree with $\Delta(T) = \Delta \geq 1$, then show that either $\lambda(T) \geq \Delta + 1$ or $\lambda(T) = \Delta + 2$. (10)

8. For every integer $n \geq 3$, show that Hamiltonian chromatic number $hc(K_{1,n-1}) = (n-2)^2 + 1$.