Course Code	Course Name	Category	L	T	P	Credit	Year of Introduction
MA0M30B	ALGEBRA AND NUMBER THEORY	BTech Minors S6	3	1	0	4	2020

i) COURSE OVERVIEW:

This is an introductory course in algebra and number theory with special emphasis on applications including RSA, prime factorization and the interplay between rings and numbers. **Prerequisite:** A basic understanding of set theory and logic**..**

ii) COURSE OUTCOMES

After the completion of the course, the student will be able to:

Course Outcomes	Description	Learning Level
CO 1	Solve number theoretic problems by applying the concept and properties of natural numbers and applications of division algorithm and related results	Apply
CO 2	Utilise the concepts and properties learned about prime numbers and basic factorisation algorithms to solve number theoretic problems	Apply
CO 3	Solve algebraic problems using the concepts and properties of groups and group structures	Apply
CO 4	Utilise the concept, properties and applications of cyclic groups, permutations and symmetric groups to solve algebraic problems	Apply
CO 5	Solve algebraic problems using the concept, properties and applications of rings and ring structures	Apply

iii) SYLLABUS

Module 1 (Elementary Number Theory) Division with remainder, congruences, greatest common divisor, Euclidean algorithm, Chinese remainder theorem, Euler's theorem

Module 2 (Prime Numbers) Prime Numbers- basic results, unique factorisation, computing Euler function, RSA explained, Fermat's little theorem, pseudoprimes, Algorithms for prime factorisationFermat's and Fermat-Kraitchik algorithms (evaluation only), Quadratic residues.

Module 3 (Introduction to Groups) Groups- Definition- basic properties and examples, subgroups and cosets, normal subgroups, group homomorphisms. Isomorphism theorem

Module 4 (Further topics in Group theory) Order of a group element, Cyclic groups, symmetric groups, cycles, simple transpositions and bubble sort, alternating groups.

Module 5 (Ring Theory) Rings- Definition, ideals, principal ideal domain, Quotient rings, Prime and maximal ideals, Ring homomorphisms, unique factorisation domain, irreducible and prime elements, Euclidean domain.

(iv) TEXT BOOKS

Niels Lauritzen, "Concrete Abstract Algebra", Cambridge University Press,2003

OTHER REFERENCES

1. David M Burton, "Elementary Number Theory", 7th edition, McGraw Hill, 2011
2. John B Fraleigh, "A first course in Abstract Algebra". 7th edition, Pearson Education India, 2013
3. Joseph A Gallian, "Contemporary Abstract Algebra", 9th edition, Cengage Learning India Pvt. Ltd

COURSE PLAN

Module	Contents	No. of hours
I	**Elementary Number Theory**-Division with remainder -Congruence- Properties of Congruence- Greatest Common divisor -Euclidean algorithm- Relatively prime numbers -Chinese Remainder Theorem- Euler's Theorem	12
II	**Prime Numbers**- Basic Results- unique factorization- Computing ϕ−function- RSA explained- Fermat's Little theorem, Pseudoprimes- Factorisation algorithms- Fermat's algorithm- Fermat-Kraitchik algorithm- Quadratic residue- Quadratic residue applications	12
III	**Introduction to Groups**- DeSinition- Basic Properties- Examples- Subgroups- Cosets- Normal Subgroups- Quotient Groups- Group homomorphisms- Isomorphism theorem	12
IV	**Further topics in Group Theory**- Order of a group element- Cyclic Groups- Properties- Symmetric groups- Cycles- Properties- Simple transpositions- Bubble sort- Alternating groups.	12
V	**Ring Theory**- DeSinition, basic properties, ideals- Quotient rings- Prime and Maximal ideals- Ring homomorphisms,- Unique factorization- Irreducible elements- prime elements- Euclidean domain	12
	Total hours	60

i) ASSESSMENT PATTERN

Bloom's Taxonomy Level	Continuous Assessment Exams (Marks)		End Semester Exam (Marks)
	CA Exam I	CA Exam II	
Remember	10	10	20
Understand	20	20	40
Apply	20	20	40
Analyse			
Evaluate			
Create			

ii) CONTINOUS ASSESSMENT EVALUATION PATTERN

Attendance	:	**10 marks**
CA Exams (2 numbers)	:	**25 marks**
Assignment/Project/Case study etc.	:	**15 marks**
Total	:	**50 marks**

iii) CONTINUOUS ASSESSMENT EXAMINATION PATTERN

- **Two tests of 50 marks** each (half the syllabus to be covered in each exam – 2 ½ modules)
- Duration – **2 hours**

iv) END SEMESTER EXAMINATION PATTERN

Duration – **3 hours**

Total marks **-100**