



ARSD College, University of Delhi

Model Course Handout/Lesson Plan

Course Name : B.Sc. (Physics Sc. Electronics)						
Semester	Course Code	Course Title	Lecture (L)	Tutorial (T)	Practical (P)	Credit (C)
VI	DSE-4 (i)	Number Theory	5	1	0	6
Teacher/Instructor(s)		SHILPI JAIN				
Session		2021-22				

Course Objective:

In number theory there are challenging open problems which are comprehensible at undergraduate level, this course is intended to build a micro aptitude of understanding aesthetic aspect of mathematical instructions and gear young minds to ponder upon such problems. Also, another objective is to make the students familiar with simple number theoretic techniques, to be used in data security.

Course Learning Outcomes:

This course will enable the students to:

- i) Learn about some fascinating discoveries related to the properties of prime numbers, and some of the open problems in number theory, viz., Goldbach conjecture etc.
- ii) Know about number theoretic functions and modular arithmetic.
- iii) Solve linear, quadratic and system of linear congruence equations.
- iv) Learn about public key crypto systems, in particular, RSA.

Lesson Plan:

Unit No.	Learning Objective	Lecture No.	Topics to be covered
1.	Distribution of Primes and Theory of Congruencies	1 and 2	Linear Diophantine equation and its solutions
		3	Distribution of primes
		4	Prime counting function, Statement of the prime number theorem
		5	Goldbach conjecture

		6	Fermat and Mersenne primes
		7 and 8	Congruence relation and its basic properties
		9 and 10	Linear congruence equation and its solutions
		11	Chinese remainder theorem
		12	to solve system of linear congruence for two variables
		13	Fermat's little theorem
		14	Wilson's theorem
		15	Revision and exercise Questions
2.	Number Theoretic Functions	16 and 17	Number theoretic functions for sum and number of divisors
		18 and 19	Multiplicative function
		20 and 21	Mobius inversion formula
		22	The greatest integer function
		23 and 24	Euler's phi-function
		25	Discussion and exercise Questions
		26 and 27	Euler's theorem
		28 and 29	Properties of Euler's phi-function
30	Revision		
3.	Primitive Roots	31 and 32	The order of an integer modulo n .
		33	Examples and Questions
		34 and 35	Theorems
		36	Primitive roots for primes.
		37 and 38	Theorems
		39 and 40	Exercise Questions
		41 and 42	Composite numbers having primitive roots.
		43 and 44	Theorems and Questions
		45	Definition of quadratic residue of an odd prime
		46	Examples
		47 and 48	Euler's criterion
		49 and 50	Revision and exercise questions
4.	Quadratic Reciprocity Law and Public Key Encryption	51 and 52	The Legendre symbol and its properties
		53 and 54	Theorems and Examples
		55	Exercise questions
		56 and 57	Quadratic reciprocity law
		58 and 59	Examples and Questions

		60	Quadratic congruencies with composite moduli.
		61 and 62	Theorems and questions
		63 and 64	Public key encryption, and.
		65 and 66	RSA encryption
		67 and 68	decryption scheme
		69 and 70	Revision and test

Evaluation Scheme:

No.	Component	Duration	Marks
1.	Internal Assessment		25
	• Quiz		
	• Class Test		
	• Attendance		
	• Assignment		
2.	End Semester Examination	3 hr	75

Details of the Course		
Unit	Contents	Contact Hours
1	<p align="center">Distribution of Primes and Theory of Congruencies</p> Linear Diophantine equation, Prime counting function, Prime number theorem, Goldbach conjecture, Fermat and Mersenne primes, Congruence relation and its properties, Linear congruence and Chinese remainder theorem, Fermat's little theorem, Wilson's theorem.	15
2	<p align="center">Number Theoretic Functions</p> Number theoretic functions for sum and number of divisors, Multiplicative function, The Mobius inversion formula, The greatest integer function. Euler's phi-function and properties, Euler's theorem.	15
3	<p align="center">Primitive Roots</p> The order of an integer modulo n , Primitive roots for primes, Composite numbers having primitive roots; Definition of quadratic residue of an odd prime, and Euler's criterion.	20
4	<p align="center">Quadratic Reciprocity Law and Public Key Encryption</p> The Legendre symbol and its properties, Quadratic reciprocity, Quadratic congruencies with composite moduli; Public key encryption, RSA encryption and decryption.	20
	Total	70
Suggested Books:		

Sl. No.	Name of Authors/Books/Publishers	Year of Publication/Reprint
1	Burton, David M. (2012). Elementary Number Theory (7th ed.). Mc-Graw Hill Education Pvt. Ltd. Indian Reprint.	2012
2	Jones, G. A., & Jones, J. Mary. (2005). Elementary Number Theory. Undergraduate Mathematics Series (SUMS). First Indian Print.	2005
3	Neville Robinns. (2007). Beginning Number Theory (2nd ed.). Narosa Publishing House Pvt. Limited, Delhi.	2007
Mode of Evaluation:		Internal Assessment / End Semester Exam

Progress Report:

Unit No.	Learning Objective	Lecture No.	Topics to be covered
1.	Distribution of Primes and Theory of Congruencies		Linear Diophantine equation and its solutions
			Distribution of primes
			Prime counting function, Statement of the prime number theorem
			Goldbach conjecture
			Fermat and Mersenne primes
			Congruence relation and its basic properties
			Linear congruence equation and its solutions
			Chinese remainder theorem
			to solve system of linear congruence for two variables
			Fermat's little theorem
			Wilson's theorem
2.	Number Theoretic Functions		Revision and exercise Questions
			Number theoretic functions for sum and number of divisors
			Multiplicative function
			Mobius inversion formula
			The greatest integer function
			Euler's phi-function
			Discussion and exercise Questions
			Euler's theorem
3.	Primitive Roots		Properties of Euler's phi-function
			Revision
			The order of an integer modulo n.
			Examples and Questions
			Theorems
	Primitive roots for primes.		
	Theorems		
	Exercise Questions		

		Composite numbers having primitive roots.
		Theorems and Questions
		Definition of quadratic residue of an odd prime
		Examples
		Euler's criterion
		Revision and exercise questions
4.	Quadratic Reciprocity Law and Public Key Encryption	The Legendre symbol and its properties
		Theorems and Examples
		Exercise questions
		Quadratic reciprocity law
		Examples and Questions
		Quadratic congruencies with composite moduli.
		Theorems and questions
		Public key encryption, and.
		RSA encryption
		decryption scheme
		Revision and test