MATH-274 Elementary Number Theory

Credit Hours: 3-0

Prerequisite: None

Course Objectives: The focus of the course is on study of the fundamental properties of integers and develops ability to prove basic theorems. The specific objectives include study of division algorithm, prime numbers, Euclidean algorithm, Congruences, Fermat and Euler's theorem, Diophantine equations, perfect numbers, primitive root theorem.

Core Contents: Divisibility and Factorization, Congruences, Arithmetic Functions, Quadratic Residues, Primitive Roots, Diophantine Equations

Detailed Course Contents: Divisibility and Factorization: Divisibility, Prime numbers, Greatest common divisors, Euclidean algorithm, Fundamental theorem of arithmetic

Congruences: Congruences, linear congruences in one variable, Chinese remainder theorem,Wilson's Theorem, Fermat's theorem, Euler's theorem

Arithmetic Functions: Arithmetic functions, multiplicative functions, Euler's Phi-function,Perfect numbers, Moebius function, Moebius inversion formula,

Quadratic Residues: Quadratic residues and non-residues, Legendre symbol, Law of quadraticreciprocity,

Primitive Roots: Order of an integer, Primitive roots for primes, Primitive root theorem Diophantine Equations: Linear Diophantine equations, Pythagorean triples, Representation ofintegers as sum of squares

Course Outcomes: Students are expected:

1. To understand the concept and properties of divisibility greatest common divisor.
2. Student's must understand and be able to use the Fermat's little theorem, Wilson'stheorem.
3. To understand and to apply the Mobius inversion formula.
4. Compute the set of all solutions to linear congruence. Be able to apply CRT and reduce general systems of linear congruences to systems studied by CRT.
5. Describe the set of all solutions to linear Diophantine equations.

Text Book: K.H. Rosen, Elementary Number Theory and its Applications, 5th edition, Addison- Wesley, 2005.

Reference Books:

1. J. K. Strayer, Elementary Number Theory, Waveland Press, INc. 2001
2. D.M. Burton, Elementary Number Theory, McGraw-Hill, 2007.

Weekly Breakdown		
Week	***Section***	***Topics***
1	1.3-1.5	Mathematical Induction, The Fibonacci Numbers, Divisibility
2	3.1	Prime numbers
3	3.3, 3.4	Greatest Common Divisors, The Euclidean Algorithm,
4	3.5, 3.6	Fundamental Theorem of Arithmetic, Factorization Methods
5	3.6, 3.7	Fermat Numbers, Linear Diophantine Equations
6	4.1 ~ 4.3	Introduction to Congruences, Linear Congruences, The Chinese Remainder Theorem
7	4.4, 4.5	Solving Polynomial Congruences, Systems of Linear Congruences
8	6.1	Wilson's Theorem, Fermat's Little Theorem
9	**Mid Semester Exam**	
10	6.2, 6.3	Pseudoprimes, Euler's Theorem
11	7.1, 7.2	The Euler Phi-Function, the Sum and Number of Divisors
12	7.3, 7.4	Perfect Numbers, Mersenne Primes, Mobius Inversion
13	9.1	Order of an Integer, Primitive Roots
14	9.2, 9.3	Primitive Roots for Primes, Existence of Primitive Roots
15	11.1,11.2	Quadratic Residues an Nonresidues, the Law of Quadratic Reciprocity
16	11.3,11.4	The Jacobi Symbol, Euler Psedudoprimes
17		Review
18	**End Semester Exam**	