

Course Outline for MATH 3111, Number Theory

MATH 3111 Number Theory (3 units)

Prerequisite: Junior standing or Mathematics major; completion of GE Area 1 with grades of C- or better; and completion of GE Area 2 with a grade of C- or better; and MATH 248 or [MATH 2031](#).

The Euclidean algorithm and greatest common divisors. Diophantine equations. Properties of prime numbers. The theory of congruences. Multiplicative functions and Möbius Inversion. Gauss' Law of Quadratic Reciprocity. Historical and modern applications of number theory. 3 lectures. Fulfills GE Areas Upper-Division 2 or Upper-Division 5.

Course Learning Objectives	
1	Formulate and prove conjectures about the integers.
2	Prove and apply the Division Algorithm.
3	Prove the Euclidean algorithm and use it to express the greatest common divisor of two integers as a linear combination of those integers.
4	Prove statements about prime numbers.
5	Use the Chinese Remainder Theorem to solve a system of linear congruences.
6	Use multiplicativity and Möbius Inversion to prove statements about number-theoretic functions.
7	Prove Euler's Theorem and use it to simplify computations in modular arithmetic.
8	Determine which integers are primitive roots modulo an integer n .
9	Use indices to solve congruence equations.
10	Use the Law of Quadratic Reciprocity to determine whether an integer is a quadratic residue modulo an integer n .
11	Describe the historical framework and applications of number theory.
12	Apply concepts from number theory to other fields, such as computer science, applied statistics, or cryptography.

Expanded Course Content

Textbooks, materials, and/or other resources
David Burton, Elementary Number Theory, 7th Edition

Week	Readings	Topics of Discussion
1	Burton Sections 1.1, 1.2	Mathematical induction, the Binomial Theorem and applications to probability, the Fibonacci sequence
2	Burton Sections 2.1, 2.2, 2.3	Foundations of number theory: the Division Algorithm, greatest common divisors, the Euclidean Algorithm
3	Burton Section 2.4	Solving Diophantine equations, examples and applications
4	Burton Sections 3.1, 3.2, 3.3	Important solved and unsolved problems about prime numbers: the Fundamental Theorem of Arithmetic, the Goldbach Conjecture. History and applications, the Sieve of Eratosthenes
5	Burton Sections 4.2, 4.3, 4.4	Congruences, representations of integers, the Chinese Remainder Theorem, examples and applications
6	Burton Sections 5.2, 5.3, 5.4	Using congruences to simplify computations in modular arithmetic; Fermat's Little Theorem, Wilson's Theorem, Fermat-Kraitchik Factorization, applications in computer science
7	Burton Section 6.1	Number theoretic functions, sum of divisors, number of divisors, multiplicativity, examples and applications
8	Burton Sections 6.2, 6.3	The Möbius Inversion formula, the greatest integer function
9	Burton Sections 7.2, 7.3	Definition and applications of Euler's phi-function, Euler's Theorem
10	Burton Sections 7.4, 8.1	Some properties of the phi-function, the order of an integer modulo n
11	Burton Sections 8.2, 8.3	Primitive roots of primes, composite numbers having primitive roots
12	Burton Section 8.4, 9.1	Definition and properties of indices, criterion for congruence solvability, Euler's criterion
13	Burton Sections 9.2, 9.3	Legendre symbol and its properties, Gauss' Law of Quadratic Reciprocity
14	Burton Sections 9.4, 10.1	Quadratic congruences with composite moduli. Introduction to Cryptography: from Caesar cipher to public key cryptography
15	Burton Sections 10.2, 10.3	The knapsack cryptosystem, an application of primitive roots to cryptography

Method of Assessment

The possible methods of assessment are written individual examinations, quizzes, in-class worksheets or presentations, projects, and homework. One or more midterms and a cumulative final exam are required.

Instructional Mode

The instructional mode for this class is face-to-face. This designation means that the essential academic standards of the course require in-class student engagement, and thus remote instruction is not appropriate.