Math 393: Introduction to Number Theory

Department of Mathematics
Millersville University

Description

Math 393 is an introduction to the theory of numbers.

Prerequisites

Math 310 (with a C- or better).

Objectives

The student will:

Demonstrate an understanding of the elementary arithmetic properties of the integers, including divisibility, congruences, modular arithmetic, and the Fundamental Theorem of Arithmetic.

Solve some Diophantine equations, congruences, and systems of congruences.

Demonstrate an understanding of fundamental results in elementary number theory, including the Euclidean algorithm, Wilson's theorem, Fermat's theorem, and Euler's theorem, the Chinese Remainder Theorem, quadratic residues, quadratic reciprocity, and continued fractions.

Apply number theory to areas such as calendars, computer science, and cryptography.

Write proofs in the context of elementary number theory.

Topics

Most of the following topics should be covered, but the instructor may make minor adjustments in coverage as appropriate.

Numbers, sequences, and sums

Induction

Fibonacci numbers

Divisibility

Primes

Greatest common divisors

The Euclidean algorithm and the Extended Euclidean algorithm

The Fundamental Theorem of Arithmetic

Factorization

Diophantine equations

Congruences

Linear congruences

The Chinese remainder theorem

Polynomial congruences

Systems of congruences

Divisibility tests

Wilson's theorem and Fermat's theorem

Euler's theorem

Euler's phi function

Divisors

Perfect numbers

Character ciphers

Block ciphers

Exponential ciphers

Public-key systems

Quadratic residues

Quadratic reciprocity

The Jacobi symbol

Decimal fractions

Finite continued fractions

Continued fractions

Periodic continued fractions

Additional topics may include: Representations of integers, computer operations with integers, complexity of operations, calendars, round-robin tournaments, hashing functions, check digits, knapsack ciphers, computer science applications, primitive roots, primitive roots for primes, existence of primitive roots, index arithmetic, primality tests, universal exponents, pseudorandom number, Mobius inversion, the ElGamal cryptosystem, Pollard's rho method, Euler pseudoprimes, splicing phone cables, zero-knowledge proofs, factoring using continued fractions, Pythagorean triples, and Pell's equation.

Recent texts

Kenneth Rosen, *Elementary Number Theorem and its Applications* (6th edition). Boston, MA: Pearson