Course Information

Math 453: Elementary Theory of Numbers (3 credits)

Course Description

Math 453 is a basic introduction to the theory of numbers. Core topics include divisibility, primes and factorization, congruences, arithmetic functions, quadratic residues and quadratic reciprocity, primitive roots and orders. Additional topics covered include sums of squares, Diophantine equations, and continued fractions.

This course satisfies the General Education Criteria for Quantitative Reasoning II.

For more details see http://catalog.illinois.edu/courses-of-instruction/math/

Course Objectives

Students should leave the course with an understanding of fundamental concepts of elementary number theory. They should also gain improved ability at reading and writing mathematical arguments. Because the subject of this course is defined more by the motivating problems than the techniques used to solve them, students should become comfortable experimenting with various approaches to problem solving and should gain experience chosing appropriate tools. Consequently, regular homework is an important aspect of the course.

Course Content

1. Divisibility and Factorization
    - Divisibility: Definition, properties, division algorithm, greatest integer function
    - Primes: Definition, Euclid's Theorem, Prime Number Theorem (statement only), Goldbach and Twin Primes conjectures, Fermat primes, Mersenne primes
    - The greatest common divisor: Definition, properties, Euclid's algorithm, linear combinations and the gcd
    - The least common multiple: Definition and properties,
    - The Fundamental Theorem of Arithmetic: Euclid's Lemma, canonical prime factorization, divisibility, gcd, and lcm in terms of prime factorizations
    - Primes in arithmetic progressions: Dirichlet's Theorem on primes in arithmetic progressions (statement only)
2. Congruences
    - Definitions and basic properties, residue classes, complete residue systems, reduced residue systems
    - Linear congruences in one variable, Euclid's algorithm
    - Simultaneous linear congruences, Chinese Remainder Theorem

- Wilson's Theorem
- Fermat's "Little" Theorem, pseudoprimes
- Euler's Theorem

3. Arithmetic Functions
   - Arithmetic function, multiplicative functions: definitions and basic examples
   - The Moebius function, Moebius inversion formula
   - The Euler phi function
   - The number-of-divisors and sum-of-divisors functions
   - Perfect numbers, characterization of even perfect numbers
4. Quadratic Residues
   - Quadratic residues and nonresidues
   - The Legendre symbol: Definition and basic properties, Euler's Criterion, Gauss' Lemma
   - The law of quadratic reciprocity
5. Primitive Roots
   - The order of an integer
   - Primitive roots: Definition and properties
   - The Primitive Root Theorem: Characterization of integers for which a primitive root exists
6. Additional topics
   - Sums of squares
   - Pythagorean triples
   - Continued fractions and rational approximations

Format

- This is an online course featuring video lectures from the UIUC Spring 2018 course taught by Professor Bruce Berndt.
- Required Text: James K. Strayer. (2002). ***Elementary Number Theory***. (2nd Edition). Waveland Press, Inc.
- Students must be able view assignments online, write out solutions, then scan or take a photo of their written work and upload it to Moodle to meet set deadlines.
- This course requires multiple exams that may be taken online.