NUMBER THEORY & CRYPTOGRAPHY

MATH/CSCI 4560/8566

Course Description:

An overview of one of the many beautiful areas of mathematics and its modern application to secure communication. The course is ideal for any student who wants a taste of mathematics outside of, or in addition to, the calculus sequence. Topics to be covered include: prime numbers, congruences, perfect numbers, primitive roots, quadratic reciprocity, sums of squares, and Diophantine equations. Applications include error-correcting codes, symmetric and public key cryptography, secret sharing, and zero knowledge proofs. **3 credits**

Prerequisites:

Undergraduates and Graduates: MATH 2230 with a C- or better or MATH 2030 with a C- or better or CSCI 2030 with a C- or better or permission of instructor

Overview of Content and Purpose of the Course:

This course is an introduction to number theory and its applications to modern cryptography. Number theory, one of the oldest branches of mathematics, is about the endlessly fascinating properties of integers. The subject is now used in public key cryptography to securely transmit information over the internet: this leads naturally to discussions of factoring, primality testing, and the discrete logarithm problem.

Specific topics to be covered include unique factorization (the Fundamental Theory of Arithmetic), divisibility criteria, the Euclidean algorithm, modular arithmetic, the Chinese Remainder Theorem, Fermat's Little Theorem and Euler's Theorem, multiplicative functions and perfect numbers, primitive roots, quadratic residues and reciprocity. Specific applications include public-key cryptography (RSA, ElGamal, and digital signatures), primality testing, discrete logarithms, secret sharing and zero knowledge proofs.

Major Topics:

1) The Integers
   a. Numbers and Sequences
   b. Sums and Products
   c. Mathematical Induction
   d. The Fibonacci Numbers
   e. Divisibility

2) Primes and Greatest Common Divisors
   a. Prime Numbers
   b. The Distribution of Primes
   c. Greatest Common Divisors and their Properties
   d. The Euclidean Algorithm
   e. The Fundamental Theorem of Arithmetic
   f. Factorization Methods and the Fermat Numbers
   g. Linear Diophantine Equations

3) Congruences
   a. Introduction to Congruences
   b. Linear Congruences
   c. The Chinese Remainder Theorem
   d. Solving Polynomial Congruences
   e. Factoring Using the Pollard Rho Method

4) Applications of Congruences
   a. Hashing Functions
   b. Check Digits

5) Some Special Congruences
   a. Wilson's Theorem and Fermat's Little Theorem
   b. Pseudoprimes
   c. Euler's Theorem

6) Multiplicative Functions
   a. The Euler-Phi-Function
   b. The Sum and Number of Divisors
   c. Perfect Numbers and Mersenne Primes

7) Cryptology
   a. Character Ciphers
   b. Block and Stream Ciphers
   c. Exponentiation Cipher
   d. Public Key Cryptography
   e. Cryptographic Protocols and Applications

8) Primitive Roots
   a. The Order of an Integer and Primitive Roots
   b. Primitive Roots for Primes
   c. the Existence of Primitive Roots
   d. Discrete Logarithms and Index Arithmetic

9) Applications of Primitive Roots and the Order of an Integer
   a. Pseudorandom Numbers
   b. The ElGamal Cryptosystem

10) Quadratic Residues

a. Quadratic Residues and Nonresidues
b. The Law of Quadratic Reciprocity
c. The Jacobi Symbol
d. Zero-Knowledge Proofs

11) Some Nonlinear Diophantine Equations

a. Pythagorean Triples
b. Fermat’s Last Theorem
c. Sums of Squares

<u>Textbook</u>:

Rosen, Kenneth H. *Elementary Number Theory and its Application, 6th ed*. London: Pearson, 2010.

May 2017