Applied Finite Mathematics

Table of Contents

1 Course Description

Course: 2030:216 Applied Finite Mathematics
Credits: 3
Prerequisite: 2030:153 Technical Mathematics III with a grade of C- or better, or placement test.
Bulletin Description: Prerequisite: 2030:153 with a grade of C- or better, or placement test. Number systems, integer rings, finite fields, number theory algorithms, prime numbers and primality tests, factoring, and random numbers.

2 Course Objectives

After completing this course the student should have the following competencies:

1. an understanding of binary, octal, and hexadecimal numbers;
2. an understanding of integer rings and finite fields;
3. the ability to use the Euclidean algorithm, the Chinese remainder theorem, Euler's ϕ function, Fermat's little theorem, and Euler's theorem;
4. an understanding of the different methods that can be used to find prime numbers;
5. an understanding of factoring algorithms and their uses;
6. an understanding of the processes used to generate random numbers.

3 Course Outline

1. Number systems
   - Representations of numbers
   - Binary, octal, and hexadecimal numbers
2. Modular arithmetic
3. Integer rings

4. Finite fields
    - Galois fields
    - Extension fields
5. Euclidean and extended Euclidean algorithms
6. Chinese remainder theorem
7. Euler's ϕ function
8. Fermat's little theorem
9. Euler's theorem
10. Prime numbers
    - Finding prime numbers: Sieve of Erastothenes etc.
    - Primality tests
11. Factoring
    - Divisibility and unique factorization
    - Factoring algorithms
12. Random numbers
    - Random and psuedorandom number generators

4 Bibliography

1. Margaret Cozzens and Steven Miller. *The Mathematics of Encryption: An Elementary Introduction*. Mathematical World, V. 29. American Mathematical Society, 2013.
2. Samuel Wagstaff. *The Joy of Factoring*. Student Mathematical Library, V. 68. American Mathematical Society, 2013.
3. Christof Paar and Jan Pelzl. *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2010.
4. Eric Gossett. *Discrete Mathematics with Proof, Second Edition*. Wiley, 2009.
5. Jeffrey Hoffstien, Jill Pipher, and Joseph Silverman. *An Introduction to Mathematical Cryptography*. Springer, 2008.
6. Shafi Goldwasser and Mihir Bellare. *Lecture Notes on Cryptography*. Available at http://cseweb.ucsd.edu/~mihir/papers/gb.html, 2008.
7. Albrecht Beutelspacher. *Cryptology*. Mathematical Association of America, 1994.