OFFICIAL SYLLABUS

MATH 315 – NUMBER THEORY

Adopted Spring 2014 (Committee: Drs. Jarosz, Voepel, Weyhaupt)

Catalog Description

Divisibility, primes, numerical functions, congruences, introduction to coding theory, continued fractions, rational approximations.

Prerequisite

Math 125 with a C or better or consent of instructor

Textbook

A Friendly Introduction to Number Theory, by Silverman, Fourth Edition, ISBN 978-0-321-81619-1, Pearson

Course Outline and Topics

Ch. 1: What is Number Theory?
Ch. 2: Pythagorean Triples
Ch. 3: Pythagorean Triples and the Unit Circle
Ch. 4: Sums of Higher Powers and Fermat's Last Theorem
Ch. 5: Divisibility and the Greatest Common Divisor
Ch. 6: Linear Equations and the Greatest Common Divisor
Ch. 7: Factorization and the Fundamental Theorem of Arithmetic
Ch. 8: Congruences
Ch. 9: Congruences, Powers, and Fermat's Little Theorem
Ch. 10: Congruences, Powers, and Euler's Formula
Ch. 11: Euler's Phi Function and the Chinese Remainder Theorem
Ch. 12: Prime Numbers
Ch. 13: Counting Primes
Ch. 14: Mersenne Primes
Ch. 15: Mersenne Primes and Perfect Numbers
Ch. 16: Powers Modulo m and Successive Squaring
Ch. 17: Computing kth Roots Modulo m
Ch. 18: Powers, Roots, and "Unbreakable" Codes

Learning Objectives

At the conclusion of this course, students should

- develop an appreciation for the role of rigorous proof in mathematics.
- be comfortable making conjectures and exploring their truth in mathematics.
- be able to identify several fundamental notions in number theory and be able to give sketches of their proofs
- be able to solve linear congruence equations, compute modular arithmetic, and use the Chinese Remainder Theorem
- understand the advantages of the RSA algorithm and be able to encrypt and decrypt using RSA
- know several classes of ``special'' numbers (such as Pythaogrean triples, Carmichael numbers, prime numbers, pseudoprimes, etc.) and their definitions
- be able to compute powers and roots in modular arithmetic efficiently