Math 346: N B◣ T ◣ (4-0-4)
June 17, 2014

Catalog Description: A proof-based course in the theory of the integers, including divisibility, primes, Euclid's Algorithm, Euler's Theorem and an introduction to algebraic structures. The course includes applications of number theory such as RSA encryption.

Prerequisite: MATH 327 with grade C or better.

Course Objectives: After completing this course, students will be able to:

1. Solve problems involving divisibility, g.c.d., Euclidean algorithm and the Fundamental Theorem of Arithmetic.
2. Use the Theory of Congruences to prove statements and solve problems.
3. Work with basic number theoretic functions.
4. Apply number theoretic concepts to cryptography.

Learning Outcomes and Performance Criteria

1. Solve problems involving divisibility, g.c.d., Euclidean algorithm and the Fundamental Theorem of Arithmetic.

   Core Criteria:

   (a) Apply the Division Algorithm.
   (b) Use the Euclidean Algorithm to find the greatest common divisor (g.c.d.) of two integers.
   (c) Use the Euclidean Algorithm to solve a Diophantine Equation of the form $ax + by = c$.
   (d) Use the Fundamental Theorem of Arithmetic to solve problems involving prime numbers.
   (e) Use the Division Algorithm and the Euclidean Algorithm to prove mathematical statements.

   Additional Criteria:

   (a) Use the Fundamental Theorem of Arithmetic to prove mathematical statements.

2. Use the Theory of Congruences to prove statements and solve problems.

   Core Criteria:

   (a) Apply basic properties of congruences to solve problems.
   (b) Solve a linear congruence of the form $ax \equiv b \mod n$.
   (c) Solve a system of linear congruences using the Chinese Remainder Theorem.
   (d) Use the Theory of Congruences to prove mathematical statements.
   (e) Use Euler's theorem, Fermat's Little Theorem, Wilson's Theorem to prove statements and solve problems.

Additional Criteria:

(a) Use Fermat's factorization method to factor integers.

3. Work with basic number theoretic functions.

   (a) Use the properties of Euler's ϕ-function to evaluate the function.
   (b) Use properties of the Greatest integer function to solve problems.

   Additional Criteria:

   (a) Use the definition of arithmetic functions such as τ (tau) and σ (sigma) and use them to solve problems.
   (b) Use Möbius Inversion Formula.

4. Apply number theoretic concepts to cryptography.

   Core Criteria:

   (a) Use simple cryptosystems.
   (b) Use RSA public key cryptography.
   (c) Write programs to create public keys.

   Additional Criteria:

   (a) Encipher matrices.
   (b) Use Fermat factorization.
   (c) Use Factor bases.