WINONA STATE UNIVERSITY

COLLEGE OF SCIENCE AND ENGINEERING

DEPARTMENT OF MATHEMATICS AND STATISTICS

**Course Outline – MATH 347**

**Course Title:** Number Theory

**Number of Credits:** 3

**Course Description:** A study of primes, divisibility, congruences, number-theoretic functions, and Diophantine equations. Prerequisites: MATH 327 - Foundations of Mathematics. Offered spring semester.

**Possible Textbooks:**

* Elementary Number Theory and Its Applications, Kenneth H. Rosen
* Introduction to Number Theory, Peter Schumer
* Elementary Number Theory, James K. Strayer
* Elementary Number Theory, David M. Burton
* Elementary Number Theory in Nine Chapters, James J. Tattersall
* An Introduction to the Theory of Numbers, Niven & Zuckerman

**Topics Covered:**

1. The Integers
   1. Divisibility
   2. Greatest common divisor
   3. The Euclidean algorithm
   4. Different bases
   5. Pythagorean triples and Fermat's Last Theorem (optional)
2. Run-Time Analysis of Number Theory Algorithms
   1. Comparison of Algorithms
   2. Order of Magnitude Analysis
3. Prime numbers
   1. Properties
   2. The Fundamental Theorem of Arithmetic
   3. Factorization methods and Fermat numbers
4. Congruences
   1. Definitions
   2. Linear congruences
   3. Linear Diophantine equations
   4. The Chinese Remainder Theorem
   5. Systems of linear congruences
   6. Solving quadratic congruences (optional)
   7. Quadratic residues and reciprocity (optional)
   8. Solving polynomial congruences
   9. Primitive roots (optional)
5. Special congruences
   1. Wilson’s Theorem (optional)
   2. Euler-Fermat Theorem
   3. Psuedoprimes (optional)
6. Multiplicative functions
   1. The Euler Phi-function
   2. The sum and number of divisors
   3. Perfect numbers and Mersenne primes
   4. Mobius inversion (optional)
7. Applications of Number Theory
   1. Divisibility Tests (optional)
   2. The perpetual calendar (optional)
   3. Round-Robin tournaments (optional)
   4. Hashing functions (optional)
   5. Check digits (optional)
   6. Cryptology (optional)
   7. Factoring using the Pollard Rho method (optional)
   8. Continued fractions (optional)
   9. Coding theory (optional)
   10. Elliptic curves (optional)

**Listing of Sections in Departmental Text to be Covered (Name and Author of Text Here):**

**Remarks:**

**Approximate Pace of Coverage:**

**Method of Instruction:** Lecture-presentation, discussion, question-answer sessions,

use of calculators/computers, group work.

**Evaluation Procedure:** Homework, quizzes, projects, midterm exams, and a final exam.

# **General Education: Mathematics/Statistics Intensive:** *The following language should appear in the syllabus for this course.*

# This is a General Education course that satisfies the Mathematics/Statistics Intensive requirement. Mathematics 347 contains requirements and learning activities that promote students' abilities to...

1. **practice the correct application of mathematical or statistical models that are appropriate to their prerequisite knowledge of those areas;**

In MATH 347, students consider problems involving the properties of integers or subsets of the integers. Frequently, it is necessary for students to conjecture what other properties may be derived from *a priori* established properties. A conjecture that is supported by a few examples does not constitute a proof. In the end, the students’ main task is to determine the validity of a conjecture for all cases through symbolic arguments and proof techniques such as induction before it can be accepted as fact.

1. **make proper use of modern mathematical or statistical methods appropriate to their level of prerequisite knowledge, to include, if statistics is used in a substantive way, the use of a statistical package with graphics capability when appropriate.**

An example of a problem in the course is the question of cryptograms and ciphers. What are some examples of systems of encoding messages? Which system is tougher to break than others? How can one construct an effective cipher system? Students find out that cipher systems lend themselves or not to break-ins by hackers based on the properties of integers and integer equations. Part of the exercise is for students to try to break encoded messages by testing the most commonly used ciphers. In the process of decoding messages (as in WWII), it will be necessary for students to enlist the aid of computers and software such as Mathematica.

**Minnesota Transfer Curriculum:** Not Applicable

**MnSCU Learning Outcomes:**

* Students will become proficient in modular computations.
* Students will reason logically with regard to the integers.
* Students will master the Euclidean Algorithm and its applications.
* Students will solve Diophantine equations.
* Students will determine the properties of arithmetic functions.

**Last Revised:** Spring 2016 by Eric Errthum