MAS2202 Course Outline

Introduction to Number Theory with Applications ....(3) (P)

Description: The course is designed as an introduction to elementary number theory, suited for scientifically oriented students interested in mathematical enrichment. The course is essentially a project-based seminar designed to integrate mathematical principles with the use of technology to enhance the performance of real world application activities. Students are tasked to present specific topics and prove various ideas with mathematical rigor. The basic topics include logic, Pythagorean triples, divisibility and the greatest common divisor, the fundamental theorem of arithmetic, congruence, Euler Phi function, the Chinese remainder theorem, Mersenne prime numbers, RSA public-key cryptosystems, introduction to cryptology and cryptography, algorithms, and spreadsheets.

General Education Learning Outcome: The primary General Education Learning Outcome (GELO) for this course is Quantitative Reasoning, which is to understand and apply mathematical concepts and reasoning, and analyze and interpret various types of data. The GELO will be assessed through targeted questions on either the comprehensive final or an outside assignment.

Prerequisite: MAC 1140 and MAC 1114 with a grade of "C" or better in each, or MAC 1147 with a grade of "C" or better, or its equivalent.

Impact Assessment: Students will gain an appreciation of some of the surprising and unexpected results encountered in Number Theory and understand how mathematics is used to provide secure means of communication, together with an understanding of its limitations, by applying the techniques of Number Theory to a variety of problems. The course applies toward the General Education mathematics requirement area B for an Associate of Arts degree. *Introduction to Number Theory* is a terminal course. It is not a prerequisite for any course, but it provides a real world setting to help students understand the importance of mathematics in today's world as well as furthering their mathematical development by tasking them to prove various theorems. The seminar nature of this course will help students develop confidence and interpersonal communication skills.

Impact Assessment: Students will gain an appreciation of some of the surprising and unexpected results encountered in Number Theory and understand how mathematics is used to provide secure means of communication, together with an understanding of its limitations, by applying the techniques of Number Theory to a variety of problems. This course applies toward the Gordon Rule mathematics requirement. The course also applies toward the General Education mathematics requirement for an Associate of Arts degree. *Introduction to Number Theory* is a terminal course. It is not a prerequisite for any course, but it provides a real world setting to help students understand the importance of mathematics in today's world as well as furthering their mathematical development by tasking them to prove various theorems. The seminar nature of this course will help students develop confidence and interpersonal communication skills.

Broad Course Objectives: This course supports the following goals of the Math Department:

- Engage students in sound mathematical thinking and reasoning. This should include students finding patterns, generalizing, and asking/answering relevant questions.

- Provide a setting that prepares students to read and learn mathematics on their own.
- Explore multiple representations of topics including graphical, symbolic, numerical, oral, and written. Encourage students to make connections among the various representations to gain a richer, more flexible understanding of each concept.
- Analyze the structure of real-world problems and plan solution strategies. Solve the problems using appropriate tools.
- Develop a mathematical vocabulary by expressing mathematical ideas orally and in writing.
- Enhance and reinforce the student's understanding of concepts through the use of technology when appropriate.

As a result of successfully completing MAS2202, students should be able to demonstrate the following:

- Analyze/interpret quantitative data verbally, graphically, symbolically and numerically.
- Communicate quantitative data verbally, graphically, symbolically and numerically.
- Appropriately integrate technology into mathematical processes.
- Use mathematical concepts in problem-solving through integration of new material and modeling.

Topical Outline with Specific Course Objectives:
The exact objectives covered under each topic will be determined by each instructor, with at least two of those listed under each to be chosen. Ideas from logic, applications and concepts of algorithms, and use of spreadsheets will be integrated throughout the course.

Because this class is being offered in a seminar style, attainment of each objective will be through student investigation using computer programs and research under guidance of the instructor, followed by students presenting their findings to the class (in oral presentations and written projects) with a focus on the application of the ideas involved, as well as students providing formal proofs of theorems where appropriate. Possible applications include encryption and cryptanalysis in the military, diplomatic and commercial domains using the RSA cryptosystem, student projects with the collaboration of COP2551 students, and dynamical systems.

I. *Linear and Nonlinear Diophantine Equations*

   A. Solve Linear Diophantine equation in two variables.
   B. Represent a Primitive Pythagorean Triples with a unique pair of relatively prime integers.
   C. Investigate the historical background of Fermat's Last Theorem.

II. *Primes and Greatest Common Divisions*

   A. Investigate the distribution of prime numbers.
   B. Represent integers in different bases.

C. Find the greatest common factor using the Euclidean Algorithm.

D. Investigate different factorization methods, such as the sieve of Eratosthenes and Fermat factorization.

E. Investigate the proof of the Fundamental Theorem of Arithmetic.

III. Congruence

A. Solve systems of linear congruences.

B. Solve systems of linear congruences with different moduli using the Chinese Remainder Theorem.

C. Be able to factor using the Pollard Rho Method.

D. Use Wilson's Theorem and Fermat's Little Theorem as the basis for primality tests and factoring algorithms.

E. Investigate Pseudo-primes.

F. Investigate Carmichael numbers.

G. Develop divisibility tests.

H. Describe how congruences are used to detect errors in strings of digits.

IV. Multiplicative Functions

A. Determine if a function is multiplicative using the Euler Phi-function.

B. Find the value of the Euler-Phi function for integers.

C. Investigate perfect numbers and Mersenne prime numbers and their connection.

D. Explore the use of arithmetical functions, the Mobius function, and the Euler totient function.

E. Investigate the Dirichlet product of arithmetical functions.

V. Cryptography

A. Learn to encrypt and decrypt a message using character ciphers.

B. Learn to encrypt and decrypt a message using Public-Key cryptology.

<u>Evaluation</u>: Each instructor will determine the specific criteria for determining the final course grade. These criteria will be delineated in the first day handout provided to each student.

<u>Commonality</u>: All instructors will use the same textbook and cover at least two objectives listed under each topic in the topical outline. A computer lab with mathematical software is provided to facilitate collaboration and the use of technology.