MATHEMATICS 324 (B1)

ELEMENTARY NUMBER THEORY

SUMMER SESSION 2011

INSTRUCTOR: I. E. Leonard, CAB 679
e-mail: eleonard@math.ualberta.ca
or isaac@math.ualberta.ca

OFFICE HOURS: M - R 10:30 - 11:00

GRADING SCHEME:

Assignments	10%
Quizzes	10%
Midterm Exam	30%
Final Exam	50%

ASSIGNMENTS: There will be 5 assignments, and you are encouraged to work together and discuss the solutions with your fellow students. Of course, the assignment that you submit for grading should be your own version, not a carbon copy of an assignment submitted by another student. Assignments are to be handed in before 5:00 pm on the date due, in the box provided on the 3rd floor in CAB. Because of the rather tight schedule during summer session, late assignments will not be accepted.

QUIZZES: There will be 5 quizzes, one each Friday for the first 5 weeks of class. The quizzes will consist of simple problems that test your understanding of the material covered during the week, and should require 10 minutes or less to complete.

EXAMINATIONS:
Midterm Examination: Monday, July 25, in class.
Final Examination: Thursday, August 11, 11:30 – 2:30, CAB 377

SOLUTIONS: Solutions to the assignments and examinations will be posted on my home page on the web:

`http://www.math.ualberta.ca/~isaac/`

TEXTBOOKS: **Required:**
Elementary Number Theory and its Applications, Sixth Edition
by Kenneth H. Rosen
Optional:
Number Theory
by George E. Andrews

CALENDAR DESCRIPTION:

MATH 324 Elementary Number Theory
Divisibility, prime numbers, congruences, quadratic residues, quadratic reciprocity, arithmetic functions and diophantine equations; sums of squares. Prerequisites: MATH 228 (or 128, 223).

Elementary Number Theory and its Applications

Topics Selected From

Appendix A: ► Axioms for the Set of Integers

Appendix B: ► Binomial Coefficients

Chapter 1: The Integers
► 1.1 Numbers, Sequences
► 1.2 Sums and Products
► 1.3 Mathematical Induction
► 1.4 The Fibonacci Numbers
► 1.5 Divisibility

Chapter 2: Integer Representations and Operations
► 2.1 Representation of Integers
2.2 Computer Operations with Integers
2.3 Complexity of Integer Operations

Chapter 3: Primes and Greatest Common Divisors
► 3.1 Prime Numbers
► 3.2 The Distribution of Primes
► 3.3 Greatest Common Divisors
► 3.4 The Euclidean Algorithm
► 3.5 The Fundamental Theorem of Arithmetic
► 3.6 Factorization Methods and the Fermat Numbers
3.7 Linear Diophantine Equations

Chapter 4: Congruences
► 4.1 Introduction to Congruences
► 4.2 Linear Congruences
► 4.3 The Chinese Remainder Theorem
4.4 Solving Polynomial Congruences
4.5 Systems of Linear Congruences
4.6 Factoring using the Pollard Rho Method

Chapter 5: Applications of Congruences
5.1 Divisibility Tests
5.2 The Perpetual Calendar
5.3 Round-Robin Tournaments
5.4 Hashing Functions
5.5 Check Digits

Chapter 6: Some Special Congruences
► 6.1 Wilson's Theorem and Fermat's Little Theorem
6.2 Pseudoprimes
► 6.3 Euler's Theorem

Chapter 7: Multiplicative Functions
► 7.1 The Euler Phi Function
► 7.2 The Sum and Number of Divisors
► 7.3 Perfect Numbers and Mersenne Primes
► 7.4 Möbius Inversion
► 7.5 Partitions

Chapter 8: Cryptology

8.1 Character Ciphers
8.2 Block and Stream Ciphers
8.3 Exponentiation Ciphers
8.4 Public-Key Cryptography
8.5 Knapsack Ciphers
8.6 Cryptographic Protocols and Applications

Chapter 9: Primitive Roots

▶ 9.1 The Order of an Integer and Primitive Roots
▶ 9.2 Primitive Roots for Primes
▶ 9.3 Existence of Primitive Roots
9.4 Discrete Logarithms and Index Arithmetic
9.5 Primality Tests Using Orders of Integers and Primitive Roots
9.6 Universal Exponents

Chapter 10: Applications of Primitive Roots and the Order of an Integer

10.1 Pseudorandom Numbers
10.2 The ElGamal Cryptosystem
10.3 An Application to the Splicing of Telephone Cables

Chapter 11: Quadratic Residues

▶ 11.1 Quadratic Residues and Nonresidues
▶ 11.2 The Law of Quadratic Reciprocity
▶ 11.3 The Jacobi symbol
11.4 Euler Pseudoprimes
11.5 Zero-Knowledge Proofs

Chapter 12: Decimal Fractions and Continued Fractions

▶ 12.1 Decimal Fractions
▶ 12.2 Finite Continued Fractions
▶ 12.3 Infinite Continued Fractions
▶ 12.4 Periodic Continued Fractions
12.5 Factoring Using Continued Fractions

Chapter 13: Some Nonlinear Diophantine Equations*

▶ 13.1 Pythagorean Triples
▶ 13.2 Fermat's Last Theorem
▶ 13.3 Sums of Squares
▶ 13.4 Pell's Equation
▶ 13.5 Congruent Numbers

Chapter 14: The Gaussian Integers

14.1 Gaussian Integers and Gaussian Primes
14.2 Greatest Common Divisors and Unique Factorization
14.3 Gaussian Integers and Sums of Squares

* Time permitting.