Math 410 – Number Theory

Course Description from Bulletin: Divisibility, congruences, distribution of prime numbers, functions of number theory, diophantine equations, applications to encryption methods. (3-0-3)

Enrollment: Elective for AM and other majors.

Textbook(s): Burton, *Elementary Number Theory*, 6th Edition, McGraw-Hill.

Other required material: Occasional handouts

Prerequisites: MATH 230 or consent of the instructor

Objectives:

1. Students will achieve command of the fundamental definitions and concepts of number theory.
2. Students will understand and apply the core definitions and theorems, generating examples as needed.
3. Students will become proficient in writing proofs in elementary number theory.
4. Students will learn about applications to cryptography.

Lecture schedule: 3 50 minute (or 2 75 minute) lectures per week

Course Outline: Hours

0. Preliminaries 1.5
   Mathematical Induction, the Binomial Theorem
1. Divisibility 2
   The Division "Algorithm", Greatest Common Divisor, the Euclidean Algorithm & Euclid's Lemma, the Diophantine Equation $ax+by=c$.
2. Primes and Their Distribution 3
   The Fundamental Theorem of Arithmetic, the Sieve of Eratosthenes, the Goldbach Conjecture & other great unknowns
3. Congruences 3
   Basics, Binary, Decimal, & base-*B* Representations of Integers and Check Digits, Linear Congruences, the Chinese Remainder Theorem
4. Fermat's Little Theorem 3
   Fermat's Little Theorem, Pseudoprimes and Carmichael Numbers, Wilson's Theorem, the Fermat-Kraitchik Factorization Method
5. Multiplicative Functions 6
   Sum of divisors sigma$\bullet(n)$, Number of divisors $\bullet(n)$, Multiplicative Functions, Mobius function and Mobius Inversion Formula, Euler $\bullet$-function, Euler's Theorem
6. Primitive Roots 3
   The Order of an Integer modulo *n*, Primitive Roots, Lagrange's Theorem, Primitive Roots of a Prime, Primitive Roots of a Composite (without full proof), Optional: Theory of Indices

7. Quadratic Reciprocity 6
   Quadratic Congruences, Quadratic Residues and Nonresidues, Euler's Criterion, the Legendre Symbol & its properties, Gauss' Lemma, Germain Primes (& primes of the form $4k+1$ and $8k-1$), the Quadratic Reciprocity Law, $(2/p)$ and $(3/p)$, Quadratic Congruences with Composite Moduli
8. Introduction to Cryptography 3
   Basics, RSA public key cryptography, the ElGamel Cryptosystem
9. Options
- Recent developments in Primality Testing and Factorization (3)
- Continued Fractions & Wiener's Attack on RSA (5)
- Certain Diophantine Equations: Pythagorean triples, Fermat's Last Theorem, sums of squares, Waring's problem (5)

10. Exams & overflow 8-10

Assessment:	Homework	10-30%
	Quizzes/Tests	20-50%
	Final Exam	30-50%

Syllabus prepared by: Michael Pelsmajer, Hemanshu Kaul, and Robert Ellis
Date: 3/17/06