THE UNIVERSITY OF CALGARY

Department of Mathematics and Statistics

Dr. R.A. Mollin

PMAT 427

Prerequisite: Pure Mathematics 315 or consent of the Division.

Required Text: **Fundamental Number Theory with Applications**, R.A. Mollin, Chapman& Hall/CRC Press, Boca Raton, New York, London, Tokyo (1997).

Suggested Additional Text: **An Introduction to Cryptography**, R.A. Mollin, Chapman& Hall/CRC Press, Boca Raton, New York, London, Tokyo (2001).

Syllabus

Topics

Chapter One — Arithmetic of the Integers: The fundamental laws. Divisibility. Prime Numbers. Applications to Computer Science.

Chapter Two — Congruences: Basics. Linear Congruences. Arithmetic functions. The Chinese remainder theorem. Polynomial congruences.

Chapter Three — Primitive Roots: Order. Existence. Indices. Applications to cryptography.

Chapter Four — Quadratic Residues: Quadratic reciprocity law. Jacobi and Kronecker symbols. Quadratic polynomials and primes. Applications to primality testing.

Chapter Five — Continued Fractions: Finite continued fractions. Infinite continued fractions. Periodic continued fractions. Continued fractions and factoring.

Chapter Six — Diophantine Equations: Sums of squares. The equation $x^2 - Dy^2 = n$. Diophantine equations of higher degree. Elliptic curves, factoring and primality testing.

Tutorials:Tutorials are held each Thursday at 13:00 in MS 317.

Grading: There will be 5 in-tutorial tests worth 10% each, and two take home exams worth 25% each. There will be no final or mid-term. The following schedule, applies for the exams and tests:

TEST#	Date	Place	Time
1	September 23	MS 317	13:00
2	October 7	M.S. 317	13:00
3	October 21	M.S. 317	13:00
4	November 4	M.S. 317	13:00
5	November 25	M.S. 317	13:00

Note that there is no tutorial on Sept. 12th.

TEST#	Date handed out	Date handed in	Date returned marked
1	October 21	October 28	October 30
2	November 27	December 4	December 6