

Pure Mathematics 427

Number Theory

Divisibility and the Euclidean algorithm, modular arithmetic and congruences, quadratic reciprocity, arithmetic functions, distribution of primes.

(see Section 3.5C of Faculty of Science [www.ucalgary.ca/pubs/calendar/current/sc-3-5.html](http://www.ucalgary.ca/pubs/calendar/current/sc-3-5.html)  
and Course Descriptions: <http://www.ucalgary.ca/pubs/calendar/current/course-main.html>)

**Reference Text:** "Fundamental Number Theory with Applications," R.A. Mollin, CRC Press, Boca Raton, New York, London, Tokyo, (1997). (not necessarily a required text)

## Syllabus

### Topics

- Ch. 1 Arithmetic of the Integers: The fundamental laws. Divisibility. Prime Numbers. Applications to Computer Science.
- Ch. 2 Congruences: Basics. Linear Congruences. Arithmetic functions. The Chinese remainder theorem. Polynomial congruences.
- Ch. 3 Primitive Roots: Order. Existence. Indices. Applications to cryptography.
- Ch. 4 Quadratic Residues: Quadratic reciprocity law. Jacobi and Kronecker symbols. Quadratic polynomials and primes. Applications to primality testing.
- Ch. 5 Continued Fractions: Finite continued fractions. Infinite continued fractions. Periodic continued fractions. Continued fractions and factoring.
- Ch. 6 Diophantine Equations: Sums of squares. The equation  $x^2 - Dy^2 = n$ . Diophantine equations of higher degree. Elliptic curves, factoring and primality testing.

\* \* \* \* \*

