

**MAT 321-1
SPRING 2010
LIST OF TOPICS**

- I. Error detection codes
 - A. UPC codes, ISBN numbers, and introduction to congruences (5.5, suppl.)
 - B. Divisibility (1.5)
 - C. Prime numbers (3.1)
 - D. Greatest common divisors (3.3)
 - E. The Euclidean algorithm (3.4)
 - F. Congruences (4.1, 4.2)

- II. Primality testing
 - A. Wilson's Theorem and Fermat's Little Theorem (6.1)
 - B. Pseudoprimes (Fermat's Test, Miller's Test) (6.2)

- III. Error correction codes
 - A. Representations of integers (2.1)
 - B. An example (suppl.)

[Test 1 will probably occur here.]

- IV. Factorization
 - A. The fundamental theorem of arithmetic (3.5)
 - B. Factoring using the Pollard rho method (4.6)

- V. Solving simultaneous congruences and applications
 - A. The Chinese Remainder Theorem (4.3)
 - B. Applications (4.3, 8.6, suppl.)

- VI. Cryptology (secret codes)
 - A. The Euler phi function (6.3, 7.1)
 - B. Character ciphers (8.1)
 - C. Exponentiation ciphers (8.3)
 - D. Public key cryptography (8.4)

[Test 2 will probably occur here.]

- VII. Random number generators
 - A. The order of an integer and primitive roots (9.1, 9.2, 9.3)
 - B. Primality tests using primitive roots (9.5)
 - C. Pseudorandom numbers (10.1)
 - D. (If time permits) The Fermat numbers (3.6)