

## COURSE OUTLINE

Math 364.3 (01) T1, 2011–2012

MWF 1.30-2.20 pm

**Instructor:** F.-V. Kuhlmann

**Office, phone and e-mail:** 210 McLean Hall, 966-6111, fvk@math.usask.ca

**Office hours:** t.b.a.

**Text:** *Elementary Number Theory* by Charles Vanden Eynden, 2nd edition, Waveland Press.

We shall study the following topics:

- (1) Well Ordering Property and induction.
- (2) Divisibility, primes, Euclidean Algorithm, Fundamental Theorem of Arithmetic.
- (3) Congruences and the Chinese remainder theorem.
- (4) Euler's Phi Function and Euler's Theorem.
- (5) Fermat's Little Theorem and Wilson's Theorem.
- (6) Applications of number theory to Public Key Cryptography.
- (7) Primality testing, Fermat and Mersenne primes.
- (8) Quadratic residues and Quadratic Reciprocity.

If time permits, other topics such as Pythagorean triples may also be included.

**Midterm exam:** one midterm exam, the date will be fixed in class.

**Marked assignments:** You may form working groups with up to three members to hand in one assignment. Make sure to take turns in writing the solutions up, and make copies of the **marked** assignments for every member of your working group.

**Distribution of marks:**

assignments: 20%

term exam: 30%

final exam: 50%

**Further literature:** *Elementary number theory, cryptography, and codes* by Maria Welleda Baldoni, Ciro Ciliberto and Giulia Maria Piacentini Cattaneo. Springer Universitext ISBN 9783540691990. Available through the library as an E-book.