Math 406 — Exam II Review

4.1. Congruences, residues, least non-negative residues, complete set of residues, modular arithmetic.

4.2. Solving linear congruences in one variable, inverses modulo m.

4.3. Systems of linear congruences, the Chinese Remainder Theorem – omit material on computer arithmetic.

4.5. Systems of two congruences in two unknowns – omit the rest.

6.1. Wilson's Theorem and Fermat's Little Theorem, their use to solve linear congruences – omit Pollard Factorization Method.

6.3. Euler's ϕ-function and Euler's Theorem, use to solve linear congruences.

7.1. Multiplicative functions, Euler's ϕ-function and computing its values, summatory functions.

7.2. The functions σ and τ giving the sum of divisors and the number of divisors, respectively, and computing their values.

7.3. Perfect numbers, Mersenne numbers and Mersenne primes, factoring Mersenne numbers (see also 4.3), omit Lucas-Lehmer Test.