Midterm 2 Study Guide

Material covered

Chapters 7 through 9, and 10.1.

- Definitions to know:
  - What it means for two numbers to be congruent modulo n. This has 3-4 variations.
  - Congruence classes.
  - How we define addition and multiplication for congruence classes.
  - The notions of ring, integral domain, field.
  - "reduced residues".
  - Euler's ϕ function.
  - Order of an element in $\mathbb{Z}_n$
- You should know all theorem and lemma statements. Especially:
  - Two numbers are congruent modulo n if and only if they have the same remainder when divided by n.
  - Addition and multiplication are well defined for congruence classes.
  - Chinese Remainder Theorem (versions 7.4.1 and 7.4.2).
  - $\mathbb{Z}_n$ forms a ring.
  - Equivalent conditions for congruence (8.2.4).
  - Which elements mod n have multiplicative inverses.
  - The only solutions to $x^2 = 1 \bmod n$ are ± 1.
  - Wilson's theorem.
  - Formulas for computing $\phi(n)$.
  - Fermat's Little Theorem.
  - Euler's Theorem.
  - Encryption/Decryption via exponentiation (9.4.1).
  - Public Key Cryptography and RSA.
  - Order of elements modulo p divides $p - 1$.
  - Order of a power of an element divides order of the element.
- Theorems you should know how to prove:
  - Why addition and multiplication are well-defined operations for congruence classes.
  - Why congruence is an equivalence relation.
  - A finite integral domain is necessarily a field.
  - $\mathbb{Z}_n$ has zero-divisors if and only if n is prime if and only if $\mathbb{Z}_n$ is a field.
  - Every invertible element is cancellable.
  - Fermat's Little Theorem.
  - Order of a power of an element divides order of the element.

Practice Problems

- Know very well all the turned-in assignments (6-8)
- Know how to do the non-optional practice problems
- Be ready for true/false questions
- Know how to compute multiplicative inverses using the Euclidean algorithm for the gcd.
- Know how to compute the common solution to a Chinese Remainder Theorem situation.
- Know how to encrypt/decrypt via addition/multiplication modulo 26.
- Know how to perform fast exponentiation.