

# Midterm 3 / Final Study Guide

## Material covered

Chapters 10, 11, 12

- Definitions to know:
  - Primitive roots
  - The discrete logarithm
  - The Diffie-Hellman protocol
  - Quadratic residues and quadratic nonresidues
  - Positive and negative residues (in the context of Gauss's lemma)
  - Definitions of  $g$  and  $T(a, p)$
  - The Legendre symbol
  - Carmichael numbers
- You should know all theorem and lemma statements. Especially:
  - There is always a primitive root modulo a prime  $p$
  - There is an element of order  $q^s$  for each  $q^s$  dividing  $p - 1$ .
  - There are  $\phi(p - 1)$  distinct primitive roots modulo  $p$ .
  - There are exactly  $(p - 1)/2$  quadratic residues and as many quadratic non-residues.
  - Legendre symbol is multiplicative
  - Euler's identity, Gauss's lemma, Eisenstein's lemma
  - The various forms of the Law of Quadratic Reciprocity  $(-1, 2, q)$ .
  - Restatement 11.3.2
  - Theorem 11.4.1
  - Visualization of Eisenstein's lemma and proposition 11.6.1
  - What the Miller-Rabin test says.
- Theorems you should know how to prove:
  - Proposition 10.2.2 about the number of roots to  $x^m - 1$  in  $\mathbb{Z}_p$ .
  - If  $a, b$  have relatively prime orders, then the order of  $ab$  is the product of those orders (lemma 10.3.5).
  - Preamble to Euler's identity (theorem 11.2.1)
  - How to use Euler's identity to determine when  $-1$  is a quadratic residue (law of quadratic reciprocity for  $-1$ , also called the quadratic character of  $-1$ ).
  - How to use Gauss's lemma to determine the quadratic character of 2.
  - Eisenstein's lemma (11.5.1).

## Practice Problems

- Know very well all the turned-in assignments (9-10)

- Know how to do the non-optional practice problems
- Be ready for true/false questions
- Know how to:
  - compute Legendre Symbols
  - find primitive roots
  - compute orders of elements
  - find elements with specific orders, given a primitive root
  - do Diffie-Hellman key exchange
  - compute the Legendre symbol using all the different ways we learned
  - use the Miller-Rabin test