Math 4400
Midterm 2 study guide

Here's a list of results you should know and things you should know how to do, organized by topic. Along with all of this stuff, you should be able to solve all the problems in Homeworks 5 through 7.

- Groups
  - Definition of a group
  - Definition of a subgroup, and checking that something is a subgroup
  - Definition of the order of a group element
  - Definition of a cyclic group
  - Definition of $G \times H$ for two groups G and H (like in Homework 5 problem 5)
  - Computing the order of $[a]$ in $\mathbb{Z}/n\mathbb{Z}$.
  - Facts about cyclic groups (mainly, $\#\langle g\rangle = o(g)$).
  - Definition of an abelian group
  - Lagrange's theorem
- Rings/Fields
  - Definition of a ring
  - Definition of a field
  - Why fields don't have zero-divisors
  - Definition of $R^\times$
  - Characterisitic of a field
- Quadratic integers/rationals
  - Definition of $\mathbb{Z}[\omega]$ when ω is a quadratic integer
  - Definition of $\mathbb{Q}[\omega]$ when ω is a quadratic rational
  - Definition of the norm of an element, i.e. $N(\alpha)$.
  - Understanding when $a + b\omega$ is invertible in $\mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$.
  - Understanding when $\mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$ is a field
- Polynomials/Homomorphisms/Isomorphisms
  - Definition of the polynomial ring $R[X]$
  - Facts about $k[X]$ when k is a field (found in section 1 of the notes about polyonomials, homomorphisms, and isomorphisms posted online)
  - Definition of a group homomorphism/isomorphism
  - Definition of a ring homomorphism/isomorphism
  - Understand how to prove that a given function between two groups/rings is a homomorphism/isomorphism
- Primes
  - Understand the proof that there are infinitely many primes congruent to 2 modulo 3
  - Lucas-Lehmer test
- Roots
  - Solving equations of the form $x^k \equiv a \mod n$.
  - Definition of an n^{th} root of unity

  - Definition of a primitive n^{th} root of unity
  - If $\#\mu_n(F) = n$, then F has $\varphi(n)$ primitive n^{th} roots
  - Recursion formula for cyclotomic polynomials: $\Phi_n(X) = \dfrac{x^n - 1}{\prod_{d|n, d\neq n} \Phi_d(X)}$, and why it works.

- Quadratic Reciprocity
  - Definition of the Legendre symbol
  - Euler's criterion
  - Why $\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right) \cdot \left(\dfrac{b}{p}\right)$
  - When is -1 a square modulo p?
  - When is 2 a square modulo p?