Math 4400
Final exam 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 homework problems.

- All the topics from the midterm 1 study guide
- All the topics from the midterm 2 study guide
- Quadratic Reciprocity
  - The quadratic reciprocity theorem:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

  - Various statements of the quadratic reciprocity theorem and why they're equivalent.
  - Using the quadratic reciprocity theorem to determine when a number is a square modulo p
- Cryptography
  - Diffie-Hellman key exchange
  - RSA encryption
  - Using RSA for digital signatures
- Miscellaneous
  - Using the Chinese Remainder Theorem to solve congruences, e.g. $x^k \equiv a \mod n$ when $\gcd(a, n) \neq 1$