Math 102—Outline for Exam 2

*Focus on Sections 4,5,6,7,9—Cryptography will **NOT** be on the exam*

Definitions and Theorems

One thing I hope you all take away from this course is a fluency in the language of number theory. To that end, you are expected to **be able to write** the definitions of the following terms and the statements of the following theorems on the exam.

- definition of the *d-function* (from Section 7)
- definition of the *σ-function* (from Section 7)
- definition of the *ϕ-function* (from Section 9)
- statement of *Theorem 1 of Section 5* ("Linear Congruences Theorem")
- statement of *Theorem 1 of Section 6* ("Fermat's Theorem")
- statement of *Theorem 2 of Section 6* ("Wilson's Theorem")
- statement of *Theorem 1 of Section 9* ("Euler's Theorem")

Problems to Practice

1. Working with basic congruences (Section 4)
   - be able to find least residues modulo m
   - be able to find solutions to congruences using a table or cleverness, e.g. $16^{85} \equiv (-1)^{85} \pmod{17}$
2. Solving linear congruences (Section 5)
   - be able to solve linear congruences or show that they have no solution
   - be able to solve a system of linear congruences with the same modulus
   - be able to solve a system of linear congruences with different moduli
     - this was the longest type of problem we had
3. Inverses (see my Section 6 Notes)
   - be able to find a^{-1} modulo m by solving $ax \equiv 1 \pmod{m}$
   - know how to use a^{-1} to solve equations
4. Using Fermat's, Euler's, and Wilson's Theorems (Sections 6 & 9)
   - *Note: I'm using "Euler's Theorem" to refer to Theorem 1 of Section 9*
   - be able to use Fermat's and Euler's Theorems to simplify powers
     - Euler's Theorem includes Fermat's Theorem so you really only need Euler's Theorem
     - when simplifying $a^k \pmod{m}$, know what to do if $(a, m) \neq 1$ (because Euler's Theorem does **not** apply)
   - be able to use Wilson's Theorem to simplify congruences with factorials
   - be able to use all three theorems in proof questions
5. Computing the d, σ, and ϕ-functions (Sections 7 & 9)
   - be able to compute $d(n)$, $\sigma(n)$, and $\phi(n)$ (usually by factoring n first)
   - know the general formulas for computing d, σ, and ϕ for use in proofs
   - know that d, σ, and ϕ are multiplicative for use in proofs
6. Practice proofs too!
   - Make sure you can reprove all proofs from the homework. I may or may not ask you to prove the exact same thing, but I will probably choose something similar.

How to study

1. Memorize the definitions and theorems listed above and practice writing them out
2. Review core topics—make sure to have a working understanding of all definitions and theorems
3. Work problems all of the way through—focus on ones similar to those from Homeworks 5–9 and the Warm-Ups
4. Practice proofs—focus on ones similar to those from Homeworks 5–9 and the Warm-Ups
5. Come talk with me if you have any questions