Math 102—Outline for the Final Exam

*Sections 1–6,9–11 (Section 7 and Cryptography and "Wilson's Theorem" will **NOT** be on the exam)*

Definitions and Theorems

I hope you all take away from this course 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 a *prime* number [Section 2]
- definition of what it means that *a is congruent to b modulo m*, i.e. $a \equiv b \pmod{m}$ [Section 4]
- definition of the *ϕ-function* [Section 9]
- definition of the *order* of an integer a modulo m, assuming that $(a, m) = 1$ [Section 10]
- definition of a *primitive root* of m [Section 10]
- definition of the *Legendre symbol* $\left(\frac{a}{p}\right)$ [Section 11]
- statement of the *GCD Theorem* [Theorem 4 of Section 1]
- statement of *Fermat's Theorem* [Theorem 1 of Section 6]
- statement of *Euler's Criterion* [Theorem 2 of Section 11]
- statement of *Quadratic Reciprocity* [Theorem 4 of Section 11]

Problems to Practice

Old Material

1. Finding primes and determining if a number is prime (Section 2)
- Lemma 4 of Section 2 is very useful

2. Solving linear Diophantine equations (Section 3)
- be able to write out all *integer* solutions (if any) to an equation of the form $ax + by = c$
  - remember, you may have to reduce it first to make sure you get *all* solutions
- know how to quickly check if $ax + by = c$ has a solution using Lemma 2 of Section 3
- be able to work with systems of equations with more than two variables
- be able to solve these in the context of a word problem too

3. 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

4. Using Fermat's and Euler's Theorems (Sections 6 & 9)
- be able to use Fermat's and Euler's Theorems to simplify powers
- be able to use the theorems in proof questions

5. Computing Euler's ϕ-function (Section 9)
- be able to compute $\phi(n)$ (usually by factoring n first)
- know the general formulas for ϕ for use in proofs

New Material

6. Orders of elements and primitive roots (Section 10)
- be able to find the order of a modulo m using a table
- be able to determine the possible orders of numbers modulo m using Theorems 1 and 2 of Section 10
- be able to determine if a is a primitive root modulo m (by computing its order and comparing with $\phi(m)$)

7. Quadratic Congruences (Section 11)
- know that $x^2 \equiv a \pmod{p}$ has a solution $\iff \left(\frac{a}{p}\right) = 1$.
- be able to determine if $x^2 \equiv a \pmod{p}$ has a solution
  - use everything: Euler's Criterion, properties of the Legendre symbol, Quadratic Reciprocity, tables...
- be able to actually find the solutions to $x^2 \equiv a \pmod{p}$ like in the homework
- be able to determine if $x^2 + bx + c \equiv 0 \pmod{p}$ has a solution (by completing the square)

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 1–11 and the Warm-Ups
4. Practice proofs—focus on ones similar to those from Homeworks 1–11 and the Warm-Ups
5. Come talk with me if you have any questions