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)*

Key Definitions and Theorems

I will **not** ask you to write down definitions and theorems on this exam, but you will have to know how to use them. Here are some of the key ones.

- 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* $(\frac{a}{p})$ [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 to focus on

1. 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
2. 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
3. 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
4. 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 to focus on

5. 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 $\phi(m)$)
6. Quadratic congruences, Euler's Criterion, and the Legendre symbol [Section 11]
   - be able to determine if $x^2 \equiv a \pmod{p}$ has a solution (which is the same as determining if $(\frac{a}{p}) = 1$)
     - 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
   - know Euler's Criterion and properties of the Legendre symbol for use in proofs

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

Instructions for the Final Exam

Points. The exam is out of **?? points**.

Due date. This take-home exam is due at **11:59**PM on **Thursday, May 14**.

Submission. Please scan each page of your exam, including this front page, and your note sheet too. You may use a camera to do this. Then upload the scan/pictures to Canvas in the assignment titled Final Exam. You can find it here: https://csus.instructure.com/courses/57912/assignments/653548

Rules for the exam.

1. You are allowed to use:
   - a basic calculator;
   - our textbook by Dudley;
   - a note sheet: one regular size sheet of paper with any notes on it you want, made before starting the exam. Please upload a scan of your note sheet with your exam.
2. You are **NOT** allowed any resources on this exam except for our course textbook and your note sheet. This includes: no book other than our textbook, no notes from class, no pictures from class, no advanced calculators, and no apps or internet resources of any kind.
3. You are **NOT** allowed to discuss the exam—in any way—with anyone other than Josh Wiscons. This includes: no talking, no texting, no posting, and no leaving notes about the exam.
4. You are **NOT** allowed to look at another person's exam or their work.
5. You are **NOT** allowed to let another person see your exam or your work.
6. Fully justify your work unless explicitly told otherwise.
7. If you have any questions about theses rules, please email me right away.

Any violation of the rules will be regarded as cheating and reported to the Sacramento State Office of Student Conduct.

Recommendations. I recommend setting aside **2 continuous, uninterrupted hours** to devote to the exam. But you can take as long as you want. Try to do this on Tuesday (which is the day of our final exam time), and then use the remaining time to finalize and submit your work. Please try hard to find a quiet place to work. Please email me if you have any questions!