Math 102—Outline for Exam 2

Focus on Sections 4,5,6,7 (only the d function), 9, Cryptography

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 the *d-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 $ax \equiv 1 \pmod{m}$
     - we did this a couple times on homework using the Euclidean Algroithm
   - 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 and ϕ-functions (Sections 7 & 9)
   - be able to compute $d(n)$ and $\phi(n)$ (usually by factoring n first)
   - know the general formulas for computing d and ϕ for use in proofs
6. Know how to decode messages using ElGamal encryption (see my Cryptography Notes)
   - Since you cannot use Wolfram Alpha on the exam, I'll make sure that all computations can be done reasonably by hand or I will tell you the relevant information.
7. 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
4. Practice proofs—focus on ones similar to those from Homeworks 5–9
5. Come talk with me if you have any questions

Instructions for Exam 2

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

Due date. This take-home exam is due at **11:59**PM on **Monday, April 27**.

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 Exam 2. You can find it here: https://csus.instructure.com/courses/57912/assignments/653546

Rules for the exam.

1. You are **NOT** allowed any resources on this exam except for one sheet of notes made before the exam. This includes: no books, no notes from class, no pictures from class, no advanced calculators, and no internet resources of any kind.
2. 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.
3. You are **NOT** allowed to look at another person's exam or their work.
4. You are **NOT** allowed to let another person see your exam or your work.
5. Fully justify your work unless explicitly told otherwise.
6. You are allowed to use:
   - a basic calculator;
   - one regular size sheet of paper with any notes on it you want. Please upload photos of your note sheet with your exam.
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 **1.5 continuous, uninterrupted hours** to devote to the exam. But you can take as long as you want. Try to do this before Monday, and then use Monday to finalize and submit your work. Please try hard to find a quiet place to work. Please email me if you have any questions!