Information for Exam 3 - Math 100, Spring 2015

Where and when: April 1, usual classroom, usual time - try to get there 5 minutes early

What you need: Pencil or pencils, Student ID. *SERIOUSLY, DON'T FORGET THESE!*

You will not be permitted to use a calculator or have any other electronics, including smartphones or smartwatches.

The exam is OPEN BOOK and OPEN NOTES.

Form: Multiple choice, 20 problems (maybe 2-3 more for extra credit)

Coverage:

Text, Chapter 4.extension, 5.extension, 16.1, 16.2. Also the lectures and notes on RSA, on solving equations mod m, and on Fermat's Little Theorem. Supplemental material connected to these from class, posted lecture notes, and videos.

Breakdown:

1-3 problems Very basic congruence mod m problems (eg, "Which of the followng are congruent to 5 mod 12?" or "What is the residue of 45 mod 8?")

2-3 problems Arithmetic mod m (eg, "What is $17 * 1234 - 77 * 9 \mod 12$?")

2-3 problems Some harder residue problems for which Fermat's Little Theorem is helpful (eg, "What is $43^{101} \mod 11$?")

1-3 problems Solving congruence equations ("Solve $ax \equiv bmodm$")

1-2 problems more conceptual problems on congruence mod m or on Fermat's Little Theorem.

1-2 problems Encode/Decode using RSA

2-3 problems Set up RSA: which would be a good value for the public key, find the private key, etc.

1-2 problems other encryption

4-6 problems Tabulate election results using plurality, Hare, Borda, Pairwise Comparison, and/or approval Voting.

1-2 problems Technical questions about voting methods (eg, how many pairwise comparisons are necessary with n choices? How many possible rankings are there?)

1-3 problems Fairness Criteria (Condorcet, IIA, Monotocity, etc). For example, you might be asked if there is a Condorcet candidate, and if so which one?

1-2 problems More conceptual questions about voting, such as on Arrow's Theorem.

Note that there is overlap, for example finding a private key in RSA requires solving a congruence equation. The exam will be out of 20, but there might bet 22-23 problems in order to give extra credit.

Many of these are time-consuming problems, so this will probably be a long exam. The less time you have to spend looking stuff up, the more likely you will be able to complete it in the time allowed. The more you practice some of the easier ones (such as arithmetic mod m), the faster you will get; you shouldn't have to spend more than a minute apiece on such problems!