Math 346 Exam 2 Review

- Exam 2 is an in-class exam.
- Exam 2 will cover Chapters 5,7,8 and assume all previous knowledge.
- You may have one sheet of notes, one side only (regular size paper, writing in at least 12 point font). You may have no more than 3 worked out problems or theorem proofs on your note sheet. You will turn in your sheet of notes with your exam.
- Study tip: Redo old homework problems (without looking at your work) and try ones that were not assigned.
- Study tip: Make a list of the main theorems proved in the research conjectures.
- Study tip: Go through old homework and note what previous facts, lemmas, and theorems you used when solving problems.
- Study tip: Do the practice problems below (Disclaimer: This is not meant to be an exhaustive set of examples of types of problems you may see on the exam.)
- Time yourself! See how many problems you can do in 50 minutes.
- Remember - with a lot of these problems you can check your answer - do so!!

Practice Problems

1. Find the smallest positive integer x that satisfies the following system of congruences:

$$x \equiv 147 \pmod{360}$$
$$x \equiv 207 \pmod{525}$$

2. Use the Chinese Remainder Theorem to find the form of all solutions to the following system of congruences(no CRT, no credit):

$$x \equiv 1 \pmod{3}$$
$$x \equiv 4 \pmod{5}$$
$$x \equiv 6 \pmod{11}$$

3. Find all distinct solutions modulo 35 to the congruence equation $15x \equiv 30 \pmod{35}$.

4. Suppose $gcd(a, 101) = 1$. What are the possible (multiplicative) orders of a modulo 101 (Hint: 101 is prime.)

5. Find $5^{151} \pmod{101}$. DO NOT use your calculator problem. Use an order argument - show work!

6. If p and q are distinct primes, prove that for any integer a, $pq \mid a^{pq} - a^p - a^q + a$.

7. Find all solutions to $x^2 \equiv 4 \pmod{35}$ (Don't guess and check - use the CRT - Hint: HWK problem Ch.7 number 23).

8. For what values of $a \pmod{20}$ (i.e. $0 \leq a < 20$) will $ax \equiv 10 \pmod{20}$ have exactly:
(a) 1 solution? (b) 2 solutions? (c) 3 solutions? (d) 5 solutions? (e) 10 solutions?

9. There were an even number of kids at the Summer Math camp. The counselor wanted to put them into groups of 10 but there were 4 kids left over. Then she tried to put them into groups of 6 but there were 2 left over. Next she tried putting them into groups of 19 but there were 17 left over. Finally she put them into groups of 37 and there were none left over. What is the smallest number of students that could have been at math camp. Use methods from these labs to solve.

10. Which integers $0 < a < 20$ have inverses modulo 20?

11. Show that $a^{20} - 1$ is divisible by 55 whenever $gcd(a, 55) = 1$.

12. Suppose $gcd(a, n) = 1$ and $ord_n(a) = k$. Prove that $ord_n(a^j) = \frac{k}{gcd(j,k)}$.

13. Use the extended Euclidean Algorithm (not your calculator program) to find $17^{-1} \pmod{49}$

14. Find the **smallest** value of x so that $5^{2012} \equiv 5^x \pmod{29}$? Show work/explain.

15. Use the Chinese Remainder Theorem to find ALL solutions ($0 \leq x < 72$) to the congruence $x^2 + 6x - 31 \equiv 0 \pmod{72}$. Show work. No CRT, no credit. Hint: Solve the equation for x modulo 8 and modulo 9 (guess and check would work), then find the answer modulo 72 using the Chinese Remainder Theorem.