

## Exam 2 Study Guide, Exam 2 is Thursday, April 21st

Exam 2 will cover sections 2.4,2.5,2.6,2.7,2.8,2.9,3.1,3.2

The exam will be in two parts, each worth approximately 50%.

**Part I: Closed book, closed notes.** For this part you should memorize and know how to use the following definitions and theorems and techniques and when to use them. You do not need to know the proofs or the Theorem, Lemma or Corollary numbers. You should learn the answers to all the iClicker questions (posted on the course web page) as noted below.

1. The technique of modular exponentiation
2. Theorem 2.25
3. Theorem 2.26
4. The definition of the order of an element modulo  $m$
5. The definition of a primitive root modulo  $m$
6. Lemma 2.3.1
7. Corollary 2.3.8
8. Theorem 2.4.1
9. Quadratic Residue
10. Quadratic Non-residue
11. Legendre symbol
12. Theorem 3.1
13. Theorem 3.4
14. iClicker questions from March x through April 15th (Note some of these will appear between April 11th and 15th.)

**Part II: Open book, open notes.** For this part you can use the text by Niven and up to  $n$  pages (2-sided) of handwritten notes you wrote yourself where  $n$  is the 7<sup>th</sup> prime number. Some of the problems will be similar to those listed below (some, but not all, of the problems listed below were homework problems). There may be other problems as well.

1. Section 2.4, problems **11,16**
2. Section 2.5, problems **2,3,4**
3. Section 2.6, problems 4,5
4. Section 2.7, problems 1,2,4,6
5. Section 2.8, problems **5,6,8,10,14,15,18,19,21,22**
6. Section 2.9, problems **1,7**
7. Section 3.1, problems **2,3,7,11**
8. Section 3.2, problems **2,3,4,9**