

Final Exam Study Guide, Spring 2011: The final exam will cover sections 1.1-3.2,4.2-4.3,5.3 in the text by Niven. The exam will be in 2 parts, each worth approximately 50%.

Part 1: 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.

1. Definitions

- a divides b
- Greatest common divisor
- Prime number
- Congruence
- Complete Residue System
- Reduced Residue System
- Euler's ϕ function
- The order of an element modulo m
- A primitive root modulo m
- Quadratic Residue
- Quadratic Non-residue
- Legendre symbol
- Definition 4.1
- Definition 4.2
- Definition 4.3

2. Theorems and Algorithms

- Division Algorithm
- 1.3
- 1.9
- 1.16
- 1.17
- 2.1
- Fermat's Little Theorem
- Euler's Theorem
- Wilson's Theorem
- Chinese Remainder Theorem.
- The technique of modular exponentiation
- Lemma 2.31
- Corollary 2.38
- Theorem 3.1
- Theorem 3.4
- Theorem 4.4
- Theorem 4.8

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 9th Mersenne Prime M_{61} . Some of the problems will be similar to those listed below (many of the problems listed below were either homework problems or problems on the study guides to previous exams). There may be other problems as well.

1. Section 1.2, problems 1,3,9,16,22,34,43
2. Section 1.3, problems 1,4,5,6,7,27
3. Section 2.1, problems 1,2,3,6,19,20,32
4. Section 2.2, problems 3,5,7
5. Section 2.3, problems 2,3
6. Section 2.4, problems 16
7. Section 2.5, problems 2,3
8. Section 2.6, problems 5
9. Section 2.7, problems 1,2
10. Section 2.8, problems 5,6,10, 15,21,22
11. Section 3.1, problems 2,3,7,11
12. Section 3.2, problems 2,3,4,9
13. Section 4.2, problems 1,6,8,10,16,20
14. Section 5.3, problems 1,2