

Math 453, Section X, Spring 2008  
HW Assignment 8, due Friday, 4/11/2008  
(Note early deadline)

**Name (print please):**

**Comments and Hints**

Many of the problems below are computational problems. In principle, these could be done by brute force (e.g., explicitly computing  $a^k \pmod m$ , for all choices of  $a$  and  $k$ , and then picking out values with a given order). However, in most cases there are theorems available that cut down the number of computations dramatically, and you should apply these theorems. The main point of these problems is not the actual calculation (nor the final answer), but the theorems and algorithms that enable one to do the computations efficiently. For the same reason, you should not use the primitive root table in the back of the book.

Most of the proofs in this set are on the easy side, generally requiring only a few lines, in conjunction with an appropriate theorem. (E.g., both parts of 5.1:7 are easy proofs.) See the problems below for additional hints.

Section 4.3 Problems: This section is all about the Quadratic Reciprocity Law (QRL), so you'll likely need to apply QRL in these problems!

**HW 8 Problems (from Sections 4.3, 5.1, 5.2, and 5.3 of Strayer)**

- |                                                                                             |                                                                                          |
|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| 1. * 4.3:28(b)                                                                              | 10. * 5.2:10(b)                                                                          |
| 2. * 4.3:28(d)                                                                              | 11. * 5.2:11(b) (Hint: You may use the fact that $r = 2$ is a primitive root modulo 37.) |
| 3. * 4.3:30                                                                                 | 12. * 5.2:12(a) (Hint: Try contradiction)                                                |
| 4. * 4.3:32 (Hint: You'll need two theorems.)                                               | 13. * 5.2:12(b) (Easy proof)                                                             |
| 5. * 4.3:36(b) (Hint: The same problem, with 3 in place of $-5$ , was worked out in class.) | 14. * 5.2:17(a) (Fermat strikes again! Hint: See an earlier problem.)                    |
| 6. * 5.1:1(b)                                                                               |                                                                                          |
| 7. * 5.1:3(c)                                                                               | 15. * 5.3:23(b)                                                                          |
| 8. * 5.1:7(a) (Easy proof)                                                                  |                                                                                          |
| 9. * 5.1:7(b) (Easy proof)                                                                  |                                                                                          |