Problem Set 3

Due: 9:00 a.m. on Wednesday, February 3

Instructions: Carefully read Sections 1.3, 1.4 and 1.5 of the textbook. Submit solutions to all of the following problems. A subset of the problems will be graded. Be sure to adhere to the expectations outlined on the sheet *Guidelines for Problem Sets*. Submit your solutions in-class or to Dr. Cooper's mailbox in the Department of Mathematics.

Exercises: From pages 47–59 of the textbook.

1. Section 1.3 #1.19, page 52
2. Section 1.3 #1.20, page 52
3. Section 1.3 #1.21, page 52
4. Use the Fast Powering Algorithm to find the last two digits of 23^{23}.
5. Section 1.4 #1.31, page 54
6. Section 1.5 #1.32(b), page 54
7. Section 1.5 #1.35, page 55 (*Hint:* Let n be the order of g modulo p. It suffices to show that $n = p - 1$. You'll want to consider g^{2q} and apply Proposition 1.29 of the textbook.)

   Note: You may use Maxima for the Fast Powering Algorithm computations. If you do so, then please still show sufficient work. In Maxima, the command to find $a \pmod{n}$ is $\mathrm{mod}(a, n)$.