# Information for Exam 1/Problem Set 5

Exam 1 will be given on Wednesday, February 17 and will cover Chapter 1 and Sections 2.1–2.7 of the textbook, inclusive. The use of books and notes will not be allowed during the exam.

The following is Problem Set 5. Solutions to this Problem Set will not be collected. However, it is highly recommended that you complete these problems in preparation for Exam 1.

*Exercises:* From pages 107–115 of the textbook.

1. Section 2.4 #2.8, pages 108–109
2. Section 2.4 #2.9, page 109
3. Section 2.5 #2.12, pages 109–110
4. Section 2.5 #2.13 parts (a) and (b), page 110
5. Section 2.5 #2.14(c), page 110
6. Section 2.6 #2.16 parts (a) and (e), page 110
7. Use Shanks' Babystep-Giantstep Algorithm to solve the Discrete Logarithm Problem

$$11^x = 21$$

in $\mathbb{F}_{71}^*$.

**Note:** You may use Maxima for tedious computations. If you do so, then please still show sufficient work. Recall that in Maxima, the command to find $a \pmod{n}$ is $\mathrm{mod}(a, n)$. Also, the command to find the greatest common divisor of two positive integers $a$ and $b$ is $\gcd(a, b)$.