Problem Set 8

Due: 9:00 a.m. on Wednesday, March 9

Instructions: Carefully read Sections 3.1, 3.2 and 3.3 of the textbook. Submit your solutions to the following problems. 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 180–191 of the textbook.

1. Section 3.1 #3.1 parts (a) and (e), page 180
2. Let p and q be distinct primes and let e and d be positive integers such that
$$de \equiv 1 \pmod{(p-1)(q-1)}.$$
Suppose further that c is an integer such that p divides c but q does not divide c. Prove that
$$x \equiv c^d \pmod{pq}$$
is a solution to the congruence
$$x^e \equiv c \pmod{pq}.$$
You may use the general fact that if $st \equiv su \pmod{n}$ then $t \equiv u \pmod{n/d}$ where $d = \gcd(s, n)$.
3. Section 3.2 #3.7, page 182
4. Section 3.2 #3.9(b), page 182
5. Section 3.2 #3.11, pages 182–183; you may assume that g is chosen such that it is not divisible by p or q.
6. Section 3.3 #3.12(b), page 183

Note: You may use Maxima for tedious computations. If you do so, then please still show sufficient work. The following commands may be helpful:

- to find $a \pmod{n}$ type the command $\text{mod}(a, n)$;
- to find the greatest common divisor of two positive integers a and b type the command $\gcd(a, b)$;
- to find the prime factorization of a positive integer n type the command $\text{factor}(n)$.