Review for Exam over Chapter 3 in CS 113

The chapter started off with pseudocode. Be able to use it to translate an algorithm from C++ to pseudocode.

The rest of the chapter was devoted to introductory number theory.

Know the division algorithm. Be able to state it.

Be able to use it in the special case when the remainder is 0. For example, $x = ky + 0$. When the remainder is 0, y actually divides into x. We write it as $y \mid x$, and again, that means that $x = ky$ for some integer k. Be able to use this to derive facts like Theorem 3.3.4 or solve problems like 11, 12, 13 0n p.131 (Exercises, not Review Exercises.)

Also, be able to use the Euclidean algorithm to find a gcd. You can use a calculator, but not one with a gcd button.

The chapter also covered the RSA encryption algorithm. Know the notation well enough to work problems like #5-9 in the Exercises (not the Review Exercises) on p. 160.

The last part of the chapter talked about modular arithmetic. Be able to do problems like in the modular arithmetic worksheet.

Some Sample Problems

1. Given a pseudocode version of the Euclidean algorithm, convert it to C++.

2. Illustrate the division algorithm for each pair of numbers (in the order given) by writing the formula with the numbers substituted into it.
   a.) (17, 3)
   b.) (12, 4)
   c.) (74, 10)

3. Circle the pairs in the list below that are made up of numbers that are relatively prime to each other.
   (5,8) (6,18) (8, 12) ((9, 15)

3.
   a.) Show that 3 divides into all multiples of 9.

   b.) Show that if 7 divides into two integers, it divides into their sum.

6. Find the gcd of 13 and 73 using the Euclidean algorithm as discussed in class.

7. For the RSA algorithm, if p = 13 and q = 19,
   a.) Compute z.

   b.) Compute ϕ.

8. Simplify.
   a.) 7 (mod 3)
   b.) (-1) (mod 7)
   c.) (3 + 9) mod 7

9. Solve each equation below. Note: Some of these have no answers; some have one answer; some have multiple answers. (What's up with that? Aren't these linear equations?)
   a.) $2x \equiv 3 \pmod 8$
   b.) $4x \equiv 8 \pmod{10}$
   d.) $2x \equiv 6 \pmod 8$

10. Calculate these expressions, using ideas similar to those I discussed in class.
   a.) $6^4 \pmod 8$
   b.) $8^9 \pmod 7$