WEEK 2 STUDY NOTES

Make sure you read the end of the week 1 notes and do the suggested exercises for Ch. 1.2. You should also check out the worksheet on Divisibility.

In class last Friday, I outlined the proof of the Division Algorithm. Since you may be asked about this on a quiz or an exam, I will post it here for you:

A. Existence
- 1. Create the candidate
  - a. Create a set that satisfies Well-Ordering
  - (Define $S = \{a - bx \mid a - bx \geq 0\}$)
    - i. Does the set consist of non-negative integers?
    - ii. Is the set non-empty?
  - Least element $a - bq = r$ is candidate.
- 2. Prove the candidate meets the criteria
  - a. By definition of q and r, clearly $a = bq + r$.
  - b. is $0 \leq r < b$?

B. Uniqueness
- 1. Assume q_1 and r_1 also satisfy the criteria, prove $q_1 = q$ and $r_1 = r$.

Now back to Chapter 1.2 (continuing form the end of the Week 1 Notes)
Notice the hypothesis of Theorem 1.3: a and b are integers, *not both zero*. Notice the difference between the phrase "not both zero", which means that one of the two numbers could be zero, and "both not zero", which means that neither number is allowed to be zero. Small differences in phrasing can be very important!

Notice the agenda for the proof of Theorem 1.3. It asserts the existence of a greatest common divisor. In the first part of the proof, a special number, called t, is shown to exist. Notice that the Well-Ordering Axiom is not applied to the set S, because S can contain negative elements. The Well-Ordering Axiom is instead applied to the subset of S consisting only of its positive elements, and it is that subset that is shown to be empty.

In the second part of the proof, t is shown to be the greatest common divisor. Notice that this section is divided into two parts: first t is shown to be a common divisor ($t \mid a$ and $t \mid b$), and then t is shown to be the gcd by showing that for any other common divisor c, $c \leq t$.

Corollary 1.4 is a handy fact, stating that any common divisor of a and b is itself a divisor of the gcd of a and b.

Theorem 1.5 seems to be stuck in as an afterthought, but it is very important, and will play a large role. Its proof is very short because it uses the powerful fact about the gcd just developed (Theorem 1.3)

You have probably seen the Euclidean Algorithm before, but now is the time to master it, and be able to compute using it. Problem #2 in Chapter 1.1 is a key part of the process. You can check your algorithm against the Euclidean Algorithm example shown on p. 11. Study the process shown on the next page for generating the gcd as a linear combination. We will be using this process often in Chapter 2.

Notice that the book does things out of order on pages 11 and 12. The Euclidean Algorithm (Thm 1.6) is stated first, and is then followed by the statement of the lemma needed to prove it (Lemma 1.7). By the way: a *lemma* is a mathematical fact which usually is of little interest in itself, but which is needed to prove a more important theorem (think of a stepping-stone).

By the end of the week, start looking at Ch. 1.3. Look at the definition of "prime integer", check some examples, and read theorem 1.8 (very important theorem!).