Day 2 Fri 9/2/2016

Questions from 1.1

Group activity: discuss reading logs.

1. Compare questions/actions
2. Choose 2 or 3 that you think are particularly interesting or effective, esp questions you were unable to answer
3. Each group member come up with one extension question – something that would take you beyond what is in the text
4. Report back to entire class

Lecture/Discussion: section 1.2

1. Overall summary – what is it about. What should we be trying to get?
    a. Concept and operation of divisibility
    b. Properties of divisibility operation
    c. Concept of GCD
    d. Properties of GCD
    e. Algorithm for computing GCD

2. Def and properties of Divisibility
    a. Definition
    b. Connection with division algorithm
    c. Suppose $a|bc$. Must it follow that a divides one of b and c?
    d. What about special numbers, 0 and 1? Can 0 be a divisor of another number? Vice versa?
    e. Any number can have only finitely many divisors. Why?
    f. If $a|b$ and $b|c$ must it follow that $a \mid c$

3. Definition and concept of GCD
    a. What if both a and b are zero?
    b. Can you formulate a definition of GCD(a,b) using set operations, like unions or intersections?
    c. How can we be certain GCD exists and is uniquely defined as long as one of the numbers a and b is nonzero?
    d. Special cases: (a,0), (a,1), (a,2a), (a,ka).
    e. Suppose $a \mid b$. What can you say about (a, b)?
    f. Suppose $t \mid a$ and $t \mid b$. What can you say about (a, b)?
    g. What does *relatively prime* mean? Why that terminology?

4. Theorem 1.3
    a. Make up an example to illustrate what the theorem says
    b. Let $a = 15$ and $b = 20$. What elements of the integers can be expressed in the form $am + bn$ using integers m and n? Hint: systematically compute

am + *bn* using all the possible combinations of *m* and *n* between -3 and 3, inclusive. What do you notice?

c. Suppose that *x* and *y* are both expressible in the form *am* + *bn*. Show that the same is true of *x+y* as well as any integer multiple of *x* and any integer multiple of *y*.

5. Corollary 1.4
   a. This is an equivalent formulation of GCD. It means that a *known* GCD must have the two properties of the theorem, and also, that we can prove something IS a GCD by demonstrating that the two conditions hold.
   b. Before looking at the proof, what organization do you expect it to have? (It is an *if and only if* theorem.)
   c. Do the two halfs of the proof in the book begin and end as you expected?
   d. (This is a way to validate the general structure of the proof.)

6. Theorem 1.5
   a. What does the theorem say? Make up an example where the theorem applies, and verify that it gives the correct conclusion. Make up an example where (*a*,*b*) is NOT 1, so the theorem does not apply. In your example does the conclusion of the theorem hold?
   b. Notice how the *ma+nb* property of the GCD makes the proof extremely short and direct. It is a simple matter to verify that the steps are valid; less easy to grasp why the proof works. This kind of proof, with short easily verified steps combining in a mysterious way is often described as being *elegant*.

7. Lemma 1.7.
   a. Overview: result says we can replace one GCD computation by another with smaller numbers by dividing the original two numbers
   b. Proof that (*a*,*b*) = (*b*, *r*) proceeds by showing that the two pairs have exactly the same sets of common divisors. Why would that show that they would have the same GCD?
   c. Using the lemma repeatedly allows us to generate a sequence of equal GCD's such as (66,18) = (18,12) = (12,6) until we reach one that is easily computed. That leads to an algorithm as stated in Theorem 1.6.
   d. Why do we need a theorem? To demonstrate that the process will definitely stop in a finite number of steps.

8. Theorem 1.6:
   a. Use the algorithm to compute the GCD of 77 and 45.
   b. In the proof, how do we know that a remainder equal to 0 must occur in a finite number of steps?

End of Day