Topics for First Math 441 Exam, Spring 2010
Here are some comments on topics covered in Math 441 in hopes they may be useful in studying for our first exam, which is on Friday, February 26. (In case you are not familiar with it, \$ is the symbol for “section”.)

• Chapter 1: Everything in this chapter comes back at some other point in the text, in more detail, but this is the only place some of the notation is defined. Based just on this chapter (and your previous knowledge) you should:
  – Recognize several useful sets of numbers, \( \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \). Be able to tell which set(s) a particular number is in.
  – Be able to show some relations are equivalence relations
  – Understand how Cantor’s “diagonalization argument”, problem E5 on page 7, shows the set of reals between 0 and 1 cannot be put into 1-1 correspondence with the counting numbers.

• Chapter 2: Officially all of the chapter’s six sections are about induction, but in fact some are really about induction as a method of proof, while others are applications of induction.
  – §2A and §2B: You certainly should be able to prove something using the appropriate form of induction. Try to develop some feel for which form would be more appropriate to use for a problem. It is very likely you will have a problem or two asking for a proof like this, but we only have the class time for the exam so actually carrying out a proof could not take too long. If I think it would take a long time to figure out how to make some proof work, or to carry out some calculations within a proof, I may give hints or outline some steps and ask you to fill them in.
  – §2C: Be sure you know what Well-Ordering is, and how to use it in proving things about \( \mathbb{N} \) or (in some cases) \( \mathbb{Z} \). Well-Ordering is defined in our text for \( \mathbb{N} \), but it gets rather casually extended to sets in \( \mathbb{Z} \) that have a lower bound.
  – §2D: Understand (a) what the Division Theorem says and on the other hand (b) how (e.g. long division) you would find the numbers it says exist. The theorem does not itself say how to find them! I will not ask you to “regurgitate” the proof of the theorem, but understanding it will help you with other proofs.
  – §2E and §2F: I will not ask you to do calculations in other bases or convert between bases. But look at the proof of Theorem 1 (page 21) and think about why the statement of the theorem includes “\( a \) a natural number \( a \geq 2 \)”: What would happen for other choices of \( a \)? If \( a \) were not a whole number?

• Chapter 3: Some of the calculations in this chapter could get quite long. I will try to make sure all problems can be done without a lot of lengthy arithmetic, so if on the exam something seems to be taking a long time you should be sure to check whether you have properly interpreted the question, whether your arithmetic is correct, and whether there is some other, shorter, way to do it.
  – The “show that” problems among E1 \ldots E11 in §3A are good things to try as examples of coming up with a proof of something fairly simple.
§3B and §3C go together: The calculations that carry out Euclid’s Algorithm in §3B are what you read backwards to find the $r$ and $s$ in Bezout’s Identity in §3C. So you should probably always think of these processes together. I won’t ask you to prove Theorem 1 (page 32) but you should be able to get from it to the Corollaries. Understand Proposition 5, and how it underlines that Bezout’s Identity does not say that $r$ and $s$ are unique.

§3D and §3E will not be on the exam.

• Chapter 4 starts out with the Fundamental Theorem of Arithmetic: The fact that it is called “fundamental” and the fact that I went through proofs in detail suggests this might be worth spending some study time on.

§4A: I won’t ask you just to repeat the proofs, but I might pick out some parts and ask you to explain them.

Assuming the numbers were not too large, you should be able to write numbers in the form $p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$. Even if it is not practical for you to find all of those primes and exponents, if you were given some or all of a factorization of $a$ and $b$ you should be able (if necessary completing the factoring) to use this form to find $(a, b)$ and $[a, b]$, or to tell if some number $c$ (also factored) divides $a$ or $b$.

I won’t ask you about Fermat Numbers.

Don’t be so taken with this way of finding $(a, b)$ that you lose track of the Euclidean Algorithm and Bezout’s Identity!

Section §4D will not be on the exam.

• Chapter 5 is the foundation for a great deal of what we do from here on. Be sure you are comfortable working with “arithmetic modulo $n$”, i.e. actually doing computations, since otherwise (a) you might waste time on the exam and (b) you will definitely be slowed down in what we have after the exam!

§5A has the definition, which is of course crucial. Propositions 1 and 2 are fundamental to understanding §5B, and the problems on pp. 64-65 are good exercise particularly with Proposition 1.

Of course the key to all of this is the fact that congruence mod $n$ is an equivalence relation, an idea we first encountered on page 4 in the text: It is a bit strange that this fact gets passed over with just a little remark at the top of page 67. If you keep in mind that some properties you have known for a long time can be expressed in this language, it will help: E.g. “odd-ness” of a number is just the property of being congruent to 1 modulo 2.

Don’t be put off by the introduction of the new term “least nonnegative residue” (never given a definition with much fanfare, just written in between two problems on page 65, but used thereafter). Before it is introduced we already have that there Proposition 1, page 64, and this term just gives a name to the “exactly one” number the proposition talks about.

A problem like E2 or E3 (p. 67) that asks a question is also implicitly asking for a proof: Among the exercises and also on the exam, you should always tell why your answer (“yes” or “no” for E2, for example) is valid.

I won’t ask you to use the “divisibility tricks” in §5C, but you should understand the proofs of the “facts” in this section.