Review Sheet for Math 20630 Exam 1

Standard Disclaimer: The following represents a sincere effort to help you prepare for our exam. It is not guaranteed to be perfect. There might well be minor errors or (especially) omissions. These will not, however, absolve you of the responsibility to be fully prepared for the exam. If you suspect a problem with this review sheet, please bring it to my attention as soon as possible, so I can fix it.

Review Session: there will be a review session devoted to this exam in Hayes-Healy 125 on Sunday, 10/4 from 6-7 PM. The usual Monday review session on 10/5 will not be held.

Format: the exam will most likely go as follows

- A page of short answer questions like "State the *well ordering principle*" or "State the definition of *integer combination*."
- A part that begins with instructions something like "Following are 8 assertions, 5 of which are false." Identify the false ones and give examples showing that they are false.
- Problems asking you to prove or compute some specific thing. I expect there to be four or five of these.

I don't promise to keep to exactly this format. However, I won't deviate much from it.

Things to know: The exam will cover the material from the first five homeworks. Following are some specific things you should know.

definitions and statements. Regarding integers, know the well-ordering principle, unique factorization theorem (i.e. fundamental theorem of arithmetic), division algorithm; know the definition of 'divides', integer combination, prime number, relatively prime, greatest common divisor, congruent modulo m, invertible modulo m. Fermat's Little Theorem. You **do not** need to know the arithmetic or order axioms for $\mathbf{Z}$ by heart. I'll provide those, if necessary. Regarding sets, know the definitions of intersection, union, difference, complement, Cartesian product, relation, equivalence relation, equivalence class. Regarding congruences, know the statement of the chinese remainder theorem and the definitions of congruent modulo m, invertible modulo m

proofs of specific theorems. Know how to prove that there are infinitely many prime numbers. Also, know how to prove that $\gcd(a, b)$ is the smallest positive integer combination of a and b.

proof skills and techniques. The only specific techniques of proof we've encountered so far are proof by contradiction, and the method for proving that two sets are equal–be prepared to use these. Remember that a proof is often easier to work out if you first write down how you'd like to begin and end it. Use the given hypotheses. Write down and try to apply the *definitions* of relevant terms and concepts. Play with specific examples in order to warm yourself up. When you're writing a proof, make sure to correctly use things like 'implies', 'there exists', 'for every', etc.

additional useful facts. If $a|b$ and $a|c$, then a divides every integer combination of b and c. If $a|bc$ and $\gcd(a, b) = 1$, then $a|c$. A linear diophantine equation $ax + by = c$ has a solution if and only if $\gcd(a, b)|c$; similar fact for linear congruences.

computational skills. Computing the b-ary expansion of an integer, computing gcd's using the Euclidean algorithm, expressing $\gcd(a, b)$ as an integer combination of a and b, solving linear diophantine equations, linear congruences and linear systems of congruences, finding multiplicative inverse modulo m.

I'm sure I've forgotten something in all this. However, I think I've got most things down.

Advice for studying: Beyond remembering the specific things I mentioned above, make sure you review the homework problems. Compare your solutions with my solutions. Solve old problems from scratch. Solve warmup problems that you haven't already tried. Solve some problems that look similar to the ones I assigned. Etc. For one thing, I regularly take test problems nearly verbatim from the homework. For another, in my opinion, solving problems is the only way to really learn and understand math.