Review Sheet for Exam 2

Format: the format of the second exam will be similar to that of the first. If there's a difference, it'll probably be that there will be a little more computation and a little less of the "state the following" and "give counterexample" type problems. I still plan to put both types of problem on the exam, though.

Things to know:

definitions and statements. prime number; 'a divides b'; prime factorization; greatest common divisor; integer combination; relation; equivalence relation (including definitions of symmetric, reflexive, transitive); equivalence class; 'a is congruent to b modulo n'; congruence class modulo n; multiplicative inverse of a modulo n; order of $\bar{a}$ in $_n$. Chinese remainder theorem; Fermat's Little Theorem. How we get from .

computational skills. Finding gcd's using the Euclidean algorithm; expressing $\gcd(a, b)$ as an integer combination of a and b; finding prime factorizations; finding integer solutions of equations of the form $ax + by = c$; arithmetic modulo n; solving multiple congruences as in the Chinese remainder theorem; finding multiplicative inverses; computing powers using Fermat's little theorem.

good topics for proofs. divisibility; greatest common denominators; congruences; rational numbers; relations.

results in the book that are useful in proofs. Lemma 6.5, Propostion 6.6, Proposition 6.7, Theorem 6.12, Division algorithm (prop 6.14), Lemma 7.19, Theorem 7.16, Corollary 7.28, Theorem 7.36. "If $a|b$ and $a|c$, then a divides any integer combination of a and c" (not explicitly stated in the book). You shouldn't remember the specific numbers attached to these results—only what they say. A good exercise is to go back through old homework and see where/how these things get used.

Advice for studying: The advice I gave concerning the first exam still applies. Let me add just a couple of things. First of all, a common way to show that "$\gcd(a, b)$ = something" is to show that "$\gcd(a, b) \leq$ something" and then that "$\gcd(a, b) \geq$ something".

On a more general note, when you have to prove a statement, go back to definitions first writing out what all the parts of the statement mean—e.g. $a|b$ means $b = ak$ for some $k \in$. Try to imagine what the first and last lines of the proof might be. If you're started on a proof and you get stuck, go back to what you're given, and see if you can't make use of it to move forward.

Remember specific examples to help reinforce definitions and theorems. For instance, remembering that $2|200000$ is a good way to remember what $a|b$ means (i.e. which is a multiple of which).