Math 3354. Fall 2010. Section 2. Basic things you need to know on the final exam.

The following list contains some of the basic definitions, theorems and algorithms discussed in the course, which you should be completely comfortable with on the final. It is not meant to cover everything you need to know for the final; instead it should be used as a self-test that can help you determine the topics you need to spend additional time on when preparing for the final.

1. Give the definition of the greatest common divisor (gcd) of two integers.
2. State the GCD theorem.
3. Describe the algorithm of computing $gcd(a, b)$ for two integers a and b and writing $gcd(a, b)$ as an integral linear combination of a and b.
4. State the basic properties of congruences.
5. Describe the algorithm for solving the linear congruence $ax \equiv b \mod n$, where a, b and n are fixed integers and $gcd(a, n) = 1$.
6. Give the definition of an equivalence relation. How would you compute the equivalence classes with respect to a given equivalence relation?
7. Define the ring $\mathbb{Z}_n$ of congruence classes modulo n.
8. Which elements of $\mathbb{Z}_n$ are invertible?
9. For which n is $\mathbb{Z}_n$ a field?
10. Give the definition of a subgroup.
11. Let G be a group and a an element of G. Give the definition of $\langle a \rangle$, the cyclic subgroup of G generated by a. Describe the practical algorithm for listing all elements of $\langle a \rangle$ (without repetitions).
12. Give the definition of a cyclic group.
13. Let $G = (\mathbb{Z}_n, +)$. Describe all generators of G and all subgroups of G (without repetitions).
14. Give two definitions of the order of an element of a group.
15. Give the definition of an isomorphism of groups.
16. If you are given two groups G and G', how would you try to show that G and G' are isomorphic? How would you try to show that G and G' are NOT isomorphic?
17. If $f : A \to B$ is a map from A to B, how would you check whether f is injective; surjective; bijective?
18. Give the definition of a homomorphism of groups. Define the kernel and the range of a group homomorphism. What are the key properties of the range and the kernel?
19. State and prove the range-kernel theorem.
20. State Lagrange theorem and its corollaries.
21. Define the permutation group S_n. If an element $f \in S_n$ is defined by the list of its values $(f(1) = \quad, f(2) = \quad, \ldots)$, how to write f as a product of disjoint cycles?
22. How to write an element $f \in S_n$ as a product of transpositions? Define the notion of an even/odd permutation.
23. Given $f, g \in S_n$, how do you compute the conjugate gfg^{-1}?
24. If H is a subgroup of a group G, how do you determine the left cosets with respect to H (so that you get a list without repetitions)?
25. Give the definition of a normal subgroup. State the conjugation criterion of normality.

26. Describe some sufficient (and easily verifiable) conditions for a subgroup H of a group G to be normal.
27. If H is a normal subgroup of a group G, describe the quotient group G/H.
28. State the fundamental theorem of homomorphisms for groups (FTH). Describe how you would try to use FTH to prove that a quotient group G/H is isomorphic to some other group Q.
29. Give the definitions of a ring, a commutative ring, a ring with unity, a field.
30. Give the definition of a subring of ring R. If X is a subset of R, describe the general algorithm for computing the minimal subring of R containing X.
31. Give the definition of an ideal I of commutative ring R. Define the principal ideal of R generated by an element $a \in R$.