Final Review, Math 305, Spring 2022

Dr Holmes

April 27, 2022

You will be allowed your single sheet of notebook paper and non-graphing calculator as on earlier exams.

My outline concept is that the inclass component of the final will have ten questions, four from Test I, four from Test II, two from new material. There might be more questions from which you can choose this many, depending on how much I dither about what to ask (or think you might benefit from having a choice).

From the Test I review, things to take special note of in boldface

axiomatics before induction: I might ask you to prove some of the more familiar order axioms (the ones for $<$) using the less familiar ones (the axioms for $\mathbb{Z}^+$).

well-ordering principle: I might ask you to prove something using the well-ordering principle. The proof that no integer is between 0 and 1 is a nice example. So is the proof that every positive integer greater than or equal to two can be factored into primes in at least one way. These are both in the notes (well, the proof about factorizations is proved by strong induction: but it is straightforward and similar by WOP: consider the smallest counterexample). I don't promise not to think of something else (every natural number is either even or odd? I won't ask for the proof of the Division Algorithm in general).

induction proofs: Expect an induction proof, probably about divisibility properties or summations. I might ask for the first factorization theorem by strong induction, the way I do it in the notes.

FINAL REVIEW: Expect one of the two things above, or a choice between them.

EEA: Be ready to do extended Euclidean algorithm computations by hand, showing the table in my preferred style. You will be asked to do this directly, and you will also need it to solve later problems.

Euclid's lemma and related things: Be ready to prove Euclid's lemma using the Bezout idenity (that is, using the extended Euclidean algorithm, or the other similar propsitions in the book or my notes, such as "if a and b are relatively prime and go into c, then ab goes into c; if you are asked to prove something using EEA or the Bezout identity, do not say anything about prime factors! see notes pp. 16, 17. I love propositions 3.7.1 and 3.7.2 (page 20 of the notes) but these are harder; if I asked for one of those it would be in a pair with one of the easier ones.

Pythagorean triples: Be ready to generate Pythagorean triples on demand. **I might ask you to show using modular arithmetic facts mod 5 that if $a^2 + b^2 = c^2$, then at least one of a, b, c is divisible by 5, and so (explain why) if (a, b, c) is a primitive Pythagorean triple, exactly one of a, b, c is divisible by 5. (NOT A HIGH PRIORITY ON FINAL REVIEW BUT I THOUGHT OF IT)**

prime theorems: Be ready to prove that there are infinitely many primes if I choose to ask this. I don't think Ill ask for any of the other theorems in full. You *should* be able to explain clearly why any number of the form $4k + 3$ has a prime factor of the form $4k + 3$.

modular calculations: You should be able to build the multiplication and/or addition table of a small modulus. You should be able to carry out calculations of powers in modular arithmetic using the method of repeated squaring. You should be able to compute multiplicative inverses in modular arithmetic using the EEA.

linear congruences: You should be able to solve them. You should probably read the proofs leading up the the Linear Congruence Theorem; it is not impossible that I might ask you to prove some part

of this. **You should be able to solve systems of two or three equations using the Chinese Remainder Theorem.**

From the second test review. Again, things for the final review are highlighted.

section 7.4-5 in Crisman: In the 7.7 exercises in Crisman, I suggest problem 9 and problem 11 as study questions. I also like problem 8.

I could also ask for simplification of an exponential in a modulus n where you can easily compute $\phi(n)$ (a small one, as the full method of computing $\phi(n)$ which I lectured on March 31 is not in your test coverage). AND NOW YOU CAN COMPUTE $\phi(n)$ FOR ANYTHING YOU CAN FACTOR

If I ask you about the Fermat and Wilson theorems (or the Legendre theorem) I will provide a statement of the theorem.

chapter 3, Judson: The formal definition of a group is examinable.

You should be ready to answer a question as to whether a familiar mathematical system, or a small finite one, is a group or not, and to say why not if it isn't.

Any of the Propositions 3.18-3.22 are legitimate targets for examination.

Be ready to prove one of 3.23 (1) and (2) by mathematical induction. Notice that there are cases involved as to whether m and n are positive or negative.

I may ask you to identify subgroups of some small group.

In Judson 3.5 exercises, I specially recommend 2, 25 (an induction proof), 31, 33, 41 (just an example of showing that an explicitly given mathematical system is a group), 51.

chapter 4, Judson: Be able to prove theorem 4.10 (proof uses number theory, the division algorithm).

Be able to use Theorem 4.13, if not prove it.

Questions recommended from 4.5 exercises: 5, 6, 8. You should be able to look at a group $U(n)$ and determine whether it is cyclic, 24, 25, 26, 29, 37 (what else can you say about such a group?)

chapter 5, Judson: Be able to convert from the array notation for permutations to cycle notation and back. Be able to convert cycle notation to a product of transpositions and identify permutations as even or odd.

Be able to compute products of permutations given in either notation.

You should understand the notations S_n, A_n, D_n for particular groups.

Recommended questions from 5.4 exercises: 1,2,3 (computation practice), 8, 9, 10.

Question for study: is a permutation of odd order an odd permutation or an even permutation? Or can it be either?

is a permutation of even order an odd permutation or an even permutation? Or can it be either?

chapter 6, Judson: Be able to compute cosets of subgroup given to you in a group given to you.

Be able to prove lemma 1 and lemma 2 in my notes, p. 53.

Know Fermat's Theorem and Euler's Theorem and be able to prove them using Lagrange's Theorem. The proof is easy of course, but conceptually important.

Recommended exercises from 6.5:

2, 5, 16 (you all had to look up this argument, I think, but having looked it up...you should know it), 17, 21.

chapter 9, Judson: Show that the relation of isomorphism between groups is an equivalence relation.

Be able to describe isomorphisms between familiar groups or small finite groups presented to you, giving actual formulas or tables of values for the isomorphism function. Be able to verify that a function from a group to a group that I give you is an isomorphism.

Be able to recognize when groups cannot be isomorphic, for example when they have different numbers of elements of some order.

Be aware of Cayley's Theorem (every group of order n is isomorphic to a subgroup of S_n). You don't have to prove it but I may come up with a question whose answer requires you to use it.

Be able to give an operation table for a small product group.

Be able to use theorem 9.17. Be aware of theorem 9.21: it might be wise to know how to prove it.

I might ask you to verify that a given group is the internal direct product of two of its subgroups (also given). If I do, I will state the conditions you need to prove.

Recommended questions in 9.4 exercises: 1, 3, 5, 12, 15, 16, 28, 31, 48, 50

chapters 10 and 13: For chapter 10, the most I might ask you to do is, given a specific group and a specific subgroup of that group, determine whether the subgroup is normal. I might to so far as to say, show that the subgroup is normal, or show that it is not normal.

For chapter 13, I might ask you to describe the abelian groups of a particular size, up to isomorphism, using Theorem 13.10.

The actual text of Test II with highlights.

1. **Use Euler's theorem to determine the last decimal digit (i.e., the remainder mod 10) of $7^{567654528}$. Briefly explain your reasoning. Hint: you can compute $\phi(10)$ simply by inspecting the remainders mod 10.**

   and also, you know how to compute $\phi(n)$ for any modulus you can factor, so the modulus can be something much more complicated than 10.

2. Wilson's theorem asserts that for any prime p, $(p-1)! \equiv_p -1$. Prove that this is false if we do not assume that the modulus is prime, by showing that $(n-1)! \not\equiv_n -1$ if $n > 1$ is composite.

3. **Show that if $a^2 = e$ for all elements of a group G, then G is abelian. Justify everything you do from the definition of a group.**

   Not this question! But some similar sort of thing.

4. **List all the subgroups of $\mathbb{Z}_{12}$ [arithmetic mod 12 with addition as the operation] (listing all elements of each subgroup).**

5. Let p and q be distinct primes. How many generators does $\mathbb{Z}_{pq}$ have? Explain why.

6. **Show that A_{10} contains an element of order 15 (there are two things to show: that there is an element of S_{10} of order 15, and that it belongs to A_{10}; you have to explain why these two things are true, not just present the permutation).**

7. Find the left and right cosets of the cyclic subgroup generated by (12) in S_3.

   The subgroup contains the identity and (12).

   The group S_3 contains the identity, (12), (13), (23), (123) and (132).

   Explain briefly why S_3 is not a cyclic group. (The explanation can be very brief!)

8. **Give multiplication tables for each of the groups $U(5), U(10), U(12)$.**

   Show that $U(5)$ is isomorphic to $U(10)$ (exhibit an isomorphism, an actual bijection from $U(5)$ to $U(10)$ with the right properties), but $U(12)$ is not (hint: talk about orders of elements of the groups).

9. Exhibit the possible isomorphism types of abelian groups of order 36.

   For each type, say what the highest possible order of an element of the group is (this will help you to see that the isomorphism types are all different).

10. **Show that the map sending each nonzero complex number $a+bi$ to $a-bi$ is an automorphism of $\mathbb{C}^*$, the group of nonzero complex numbers under multiplication. An automorphism of the group G is an isomorphism from G to G. Reminder: this isn't just showing that the map is a bijection – you have to show its relation to the group operation, too.**

11. Show that $\{id, (123), (132)\}$ is a normal subgroup of S_3 (very briefly say what the factor group is), and that $\{id, (12)\}$ is not.

You may use the fact that a subgroup is normal iff its left cosets are the same as its right cosets.

12. Prove that each subgroup of a cyclic group is cyclic. This will use the well-ordering principle and the division algorithm from number theory.

    You may assume the properties of exponents as they apply to groups.

From new material, a few items:

1. **Be able to do hand calculations for RSA (no formulas supplied, you should know them) or for El Gamal (formulas will be on your paper, though without explanations, as a reminder)**

2. **Be able to tell whether a given number is a Carmichael number.**

   Be able to prove that a product of distinct primes which satisfies Korselt's Criterion is a Carmichael number. The actual proof that simply 561 is a Carmichael number is about as good and a bit more concrete. Be able to prove that there are infinitely many primes of the form $4n+1$. I remarked that I might ask a question where I ask you to prove one of these two things.

3. **Be able to take a square root in a modulus which is prime of the form $4n+3$. Be able to solve a quadratic equation in such a modulus.**