Math 287 Test II review

Dr Holmes

April 6, 2022

The test is on Thursday April 7.

It covers material in pp. 43-62 in the Art of Proof and pp. 16-53 in the notes.

It should have somewhere between 8 and 10 questions. I do not think I'll repeat the experiment of handing you a takehome copy. As you will see from the description, there will be more computational tasks on this test, but there will still be proofs.

strong induction and Fibonacci-like recursion: Be ready for something like the induction proof about a recursive sequence which is given on p. 16 in the notes. It might involve the actual Fibonacci sequence or, as in this case, a different recursively defined sequence.

basic set axioms and definitions: I'm not going to examine you on axioms of set theory.

The second theorem on p. 20 (transitivity of the subset relation), you should be able to write.

The proof strategy for showing that two sets are equal is important to remember. I might give you a direct example (something like project 5.3), or it might show up in connection with another problem (p. 23 of the notes for the proof strategy)

In Homework 6, you will definitely see a test question like problem 3, 4 (Venn diagrams). You should be ready to give a counterexample (small finite sets) if I propose that you prove something using Venn diagrams that is not true.

I am not going to ask for a proof about Cartesian products (like problems 6,7); the test is going to be long enough without.

functions and relations: I may draw arrow diagrams and ask you whether they are pictures of functions, and if so whether they are pictures of one-to-one functions or functions onto a given set.

I may ask questions like question 1-3 in Homework 7. If I ask you how many functions there are from a set A with 10 elements to a set of 3 elements, you can't answer it by listing but you should be able to tell how many. How many functions are there from B to A in this case?

Be ready to prove that $\equiv_n$ is an equivalence relation (in general, or for a specific n). Notice that the proof for $\equiv_3$ appears on pp. 32-3 of the notes without using the notation for congruence.

I might ask you whether other familiar relations are equivalence relations (you should be able to show which properties fail if they are not, by giving counterexamples).

Be ready to prove that if two equivalence classes meet, they are the same class (p. 34). Basic definitions will be provided if I ask this.

Be ready to describe the equivalence classes under a relation $\equiv_n$ or the equivalence classes under a relation given as a small finite set of ordered pairs.

division algorithm and Euclidean algorithm: Be ready to compute $a\texttt{div}b$ and $a\texttt{mod}b$ for values I present to you. Be sure that you know how to do this when a is negative.

Be ready to prove that the gcd of a and b is the same as the gcd of b and $a\texttt{mod}b$. This is on p. 38 of the notes. Notice that it is a proof that two sets are equal, using the proof strategy mentioned above.

Be ready to carry out the extended Euclidean algorithm (find $\texttt{gcd}(a, b)$ and integers x, y such that $ax + by = \texttt{gcd}(a, b)$) in the table format i have used, using your non-graphing calculator. I strongly suggest practice.

Modular arithmetic: As noted already, be ready to prove the theorem at the bottom of page 39, that congruence mod n is an equivalence relation.

The list of equivalence classes at the top of p. 41 is a sort of thing you should be able to produce.

Be ready to prove that if $a \equiv_n a'$ and $b \equiv_n b'$ than $ab \equiv_n a'b'$.

Be ready to compute modular addition and multiplication tables, and a table of multiplicative inverses.

Nothing like questions 6,7 in homework 8 will appear on the test. We have enough to do with the direct stuff.

You should be ready to prove Euclid's Lemma or the theorem which follows it (p. 45).

You should be able to compute a multiplicative inverse in any modulus using the Euclidean algorithm, or tell me why it doesn't exist.

You should be able to solve an equation like example 2 on p. 46.

You should be able to do a problem like example 2 on p. 48.

You should be ready to do a problem like either part of problem 5, homework 9.

You should be ready to do a problem on RSA encryption and decryption. I reserve the right to ask you to carry out the entire process (encode a message, find decryption exponent, decode the message). I'll try to have nice numbers, and I may ask questions about RSA which ask you to do only part of the process or supply you with useful information to help you do it more efficiently.

I strongly suggest practice on RSA. I point out that you can create examples yourself, and you can tell if you are doing it right, if the decryption recovers your original message. It would be natural to work in pairs on such practice; each student make a key, tell the other student their public key, and then each student send the other a coded message, which the receiver can then decode...