Math 189 Fall 2021 Test III Review

Dr Holmes

December 10, 2021

Test III (with the exception of two problems included in the take home exam) will be given in the final exam period, which is Monday December 13, 12-2 pm.

I summarize sections covered and indicate what to review, including listing some problems whose solutions will be open to you.

I am quite clearly not going to ask everything suggested here. You should expect two to four questions (possibly with parts) on each of the chapters covered. I'm definitely not going to ask four questions about each chapter: I would like to have fewer than ten numbered questions.

8.2: I may ask some simple question testing the ability to read recursion relations and compute values in recursive sequences. I opened solutions to 8.2.1 bdf.

8.4/5: Expect an induction proof question with two parts, both of which will likely either be problems you have seen or done yourself, or very similar to such problems, one a summation problem and one not. These will not involve inequality proofs.

The part you do better on will count as 70 percent of the problem and the other as 30 percent.

I opened 8.4.1g, 8.4.2 acde, 8.5.1 bcef.

8.7: The section on loop invariants will not be examined. Thank you to the students who did the homework on this: I have to think about how to ask questions about this material on tests in the future, because eventually I do want to teach it and test it.

9.1: There may be some simple question about the division algorithm theorem. The computational questions in the homework would be relevant: opened 9.1.3 efgh 9.1.4 ab. 9.1.5 ad. Simple proofs about divisibility appear in 9.1.6: I opened solutions to acf.

9.2: Do calculations in modular arithmetic. Make operation tables for small moduli.

I opened 9.2.1 bcd, 9.2.2, 9.2.4 (but they don't actually give the tables that exist: I may post them).

9.5: I strongly suggest using my table format for actual calculations.

For any positive integers m, n be able to find integers x, y such that $mx + ny = \texttt{gcd}(m, n)$.

For any a relatively prime to n, be able to find the multiplicative inverse of a in mod n arithmetic.

I opened 9.5.1cd, but I do not recommend their solution format. My table format is much more practical. You might want to practice doing it by hand (and check using my spreadsheet). I opened 9.5.2bc, but again, I do not recommend their solution format.

I opened the solutions to 9.4.4 and 9.4.5. I might ask some kind of relatively easy proof question testing understanding of the definition of the gcd (as both of these actually are doing), or I might not.

9.7: Be able to compute exponentials in modular arithmetic by repeated squaring. You may use my method or theirs. I opened all solutions to 9.7.2. I suggest practicing calculations by hand then checking against my spreadsheet.

9.9: I will ask some kind of RSA algorithm question in which hopefully the calculations will remain manageable.

I opened 9.9.1 and 9.9.4.

chapter 10: In chapter 10, you should take the problems I actually assigned as models. I will open solutions to these problems (or some of them) by Sunday, as I grade homework.

I may ask you questions involving simply evaluating permutation numbers and binomial coefficients.

10.3: I like 10.3.3.

10.4: I like 10.4.1 and we discussed it thoroughly. If I asked you a question, it would be about small sets. I like 10.4.2 and 10.4.3.

10.5: I like 10.5.5 and 10.5.7.

10.6: I like 10.6.2 and 10.6.3 but I would really like problems in which the numbers could be conveniently computed.

10.8: 10.8.1 is the exact kind of question I will ask.

10.9: 10.9.2, 10.9.3, 10.9.4 are all model questions. I'm likely to ask just the basic question (part a in each), not the refinements, though it doesn't hurt at all to think how to answer the questions with extra conditions Im also likely to use small numbers and ask you to compute actual numbers, not leave them as binomial coefficients as the book does.