Test I review, Math 305, spring 2022

Dr Holmes

February 14, 2022

To begin with, every test question will be on material we have actually discussed in class or worked on in homework.

Most but not all test questions should have some resemblance to things we did in homework: I reserve the right to ask questions designed to make you think,

There should be 8 questions on the exam. Some may appear in pairs, of which the one on which you do better will count 70 percent of the total grade and the one you do worse on 30 percent. This exam contains a fair amount of computation content which may not be appropriate to organize in this way. The instructions at the head of the exam will make it clear which questions if any are paired.

I list topics to study or skills to practice.

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.

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.

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.