Discrete Math Exam 2

Monday, April 10, 2023

The exam will take place in class on Monday, April 10. You are **not** allowed to bring any notes, textbooks, or any other resources with you to the exam, and you may not use a phone (not even as a calculator). Bring only something to write with. I will provide a fresh copy of the exam with space for writing your solutions. I will also make scratch paper available if you need it. You may use a calculator.

This exam has two parts: a "take-home" part and an "on sight" part.

- For the "take-home" part, the questions shown here are the exact same questions you will see on the exam. You may prepare your solutions ahead of time using **any resources** including textbooks, other students and professors, previous quizzes and homeworks, or any sources on the Internet. You may also ask me for feedback on potential solutions, though I will not give hints for exam questions. Of course, I am happy to answer general questions, go over homework problems, or answer clarifying questions about exam problems.
- For the "on sight" part, you will not have access to the problems in advance. However:
  - The problems will be similar to problems you have done on homework assignments. The only difference is that some problems may involve synthesizing multiple concepts or skills from the course so far instead of only focusing on one concept or skill.
  - You should create practice problems and submit them, so I can share them with the class!

Topics covered by the exam:

- Divisibility
- The division algorithm, quotient and remainder
- Modular equivalence
- Primes
- GCD and the Euclidean Algorithm
- Bézout's Theorem and the Extended Euclidean Algorithm
- Modular inverses
- Fermat's Little Theorem

Take home problems

For each proposition, state whether it is true or false, and either prove or disprove it as approrpiate.

1. The divides relation, $a \mid b$, is transitive.
2. For all integers a and b and all positive integers k and m, if $ka \equiv_m kb$ then $a \equiv_m b$.
3. If n is composite, then it has a prime divisor which is $\leq \sqrt{n}$.