Math 55, Discrete Mathematics—Spring 2021
Midterm Exam 2

Instructions

The due deadline for this exam is Tuedsday, April 6 at 8:00pm PDT. This is a firm deadline! Be sure to finish your work with enough time to spare for submitting it.

Points will be deducted for late submissions. Gradescope will not accept any submissions after 11:59pm.

The exam is to be completed in a single 80 minute session at any time during the 24-hour window from the release time to the due time. The 80 minute time limit is not enforced, but please do your best to honor it. I have tried to design the exam so that 80 minutes should be enough to demonstrate your knowledge.

If you need to take a few extra minutes to finish answering a question or questions that you know how to solve, that is OK. You should not attempt to use the unenforced time limit as a way to cram in extra studying after seeing the questions. Doing so would be stressful and unlikely to significantly improve your score.

You can write answers on paper and scan in PDF format (best) or take pictures (usually lower image quality, so be sure they are readable). You can also write answers on a tablet if you have one, and save them in PDF format.

When you submit your answers, Gradescope will ask you to indicate the page or pages where your answer to each question is located. Gradescope will let you indicate one or multiple questions on each page.

This exam is open book. You may consult the textbook, your own notes, and any other books and non-interactive web resources. Calculators are allowed, but it should be possible to answer all questions doing arithmetic by hand. You may not receive assistance from another person, or give assistance, or use web resources that provide answers to questions interactively.

There are 7 questions, for a total of 100 points. Questions are on the next page.

UC Berkeley Honor Code

"As a member of the UC Berkeley community, I act with honesty, integrity, and respect for others."

• If a question has a numerical answer, show enough work so that we can see how you arrived at your answer.
• Leave answers involving expressions such as factorials and binomial coefficients in unsimplified form.
• If a question asks you to prove or show something, your answer should be a logical argument written out in complete sentences.

Question 1 (14 points). Solve the congruence

$$17x + 57 \equiv 22 \pmod{100}.$$

Question 2 (14 points). Solve the system of congruences

$$\begin{aligned} x &\equiv 7 \pmod{15}, \\ x &\equiv 10 \pmod{32}. \end{aligned}$$

Question 3. (a) (8 points) Suppose p is a prime number other than 2 (so p is odd). Show that for every integer a not divisible by p, if the congruence

$$x^2 \equiv a \pmod{p}$$

has a solution, then $a^{(p-1)/2} \equiv 1 \pmod{p}$.

(b) (7 points) Suppose that the prime number p in part (a) has the form $p = 4k + 3$, where k is an integer. Show that if $a^{(p-1)/2} \equiv 1 \pmod{p}$, then $x \equiv a^{k+1} \pmod{p}$ is a solution of the congruence in part (a).

Question 4 (14 points). How many 13 card bridge hands have a 4-4-3-2 distribution—meaning the hand contains 4 cards from each of two suits, 3 cards from a third suit, and 2 cards from the remaining suit?

Question 5 (14 points). How many permutations of the 26 letters A–Z are there with A and Z not next to each other?

Question 6 (14 points). I use RSA with public key (n, e) to let people send me securely encrypted messages. Imagine that you are a hacker and have succeeded in finding the prime factorization $n = p\,q$ of the modulus in my public key. You also manage to intercept an encrypted message x that was sent to me. Explain what steps you would now take to decrypt the message. It is not necessary to explain in detail the steps of any algorithms you would use.

Question 7 (15 points). Prove the identity

$$f_1 + \cdots + f_n = f_{n+2} - 1$$

for all $n \geq 1$, where f_n is the n-th Fibonacci number.