CS 70 Discrete Mathematics and Probability Theory
Summer 2025 Tate Midterm

PRINT Your Name: _____, _____
(last) (first)

PRINT Your Student ID: _____

PRINT Your Exam Room: _____

SID of the person sitting to your left: _____

SID of the person sitting to your right: _____

SID of the person sitting in front of you: _____

SID of the person sitting behind you: _____

Read This.

- There will be no clarifications. We will correct any mistakes post-exam in as fair a manner as possible. Please just answer the question as best you can and move on even if you feel it is a mistake.
- Due to the above. Please move on. There are lots of problems to get points from. Do not get stuck. This is good advice anyway. In fact, we repeat it below.
- Anything written outside the boxes provided will not be graded.

Advice.

- The questions vary in difficulty. In particular, the exam is not in the order of difficulty and quite accessible short answer and proof questions are late in the exam. All blanks are worth 3 points each unless otherwise specified. No points will be given for a blank answer, and there will be no negative points on the exam. **So do really scan over the exam.**
- The question statement is your friend. Reading it carefully is a tool to get to your "rational place".
- You may consult only *one sheet of notes on both sides*. Apart from that, you may not look at books, notes, etc. Calculators, phones, computers, and other electronic devices are NOT permitted.
- **You may, without proof, use theorems and lemmas that were proven in the notes and/or in lecture, unless otherwise stated. That is, if we ask you to prove a statement, prove it from basic definitions, e.g., "$d \mid x$ means $x = kd$ for some integer k" is a definition.**
- There are a total of 255 points on this exam.

1. Pledge

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

In particular, I acknowledge that:

- I alone am taking this exam. Other than with the course staff, I will not have any verbal, written, or electronic communication about the exam with anyone else while I am taking the exam or while others are taking the exam.
- I will not refer to any books, notes, or online sources of information while taking the exam, other than what the instructor has allowed.
- I will not take screenshots, photos, or otherwise make copies of exam questions to share with others.

SIGN Your Name: _____

2. Propositional Logic

1. Let P and Q be propositions. "True" means always true, "False" means always false, and "Could be either" means it depends on the values of P and Q.

   (a) $(P \wedge \neg P) \implies Q$

   ◯ True ◯ False ◯ Could be either

   (b) $P \implies (Q \vee \neg Q)$

   ◯ True ◯ False ◯ Could be either

   (c) $(P \vee \neg P) \implies (Q \wedge \neg Q)$

   ◯ True ◯ False ◯ Could be either

   (d) $(P \vee Q) \implies (P \wedge Q)$

   ◯ True ◯ False ◯ Could be either

2. For each pair of statements below, indicate whether the two are equivalent or not.

   (a) $\forall x[P(x) \implies \exists y\, Q(x,y)]$ and $\forall x \exists y[P(x) \implies Q(x,y)]$

   ◯ Equivalent ◯ Not equivalent

   (b) $\exists x[P(x) \implies \forall y\, R(x,y)]$ and $\forall x[P(x) \vee \exists y\, R(x,y)]$

   ◯ Equivalent ◯ Not equivalent

3. Let $P(x)$ and $Q(x,y)$ be predicates, and define $R(x) = \neg P(x)$ and $S(x,y) = \neg Q(x,y)$. Rewrite the following proposition without using any "not" operators:

$$\neg(\forall x P(x) \wedge \exists x \forall y Q(x,y))$$

3. Short Proofs

1. (8 points) Prove that for $a, b, c \in \mathbb{Z}$, if $2b + 3c$ is not divisible by a, then b or c is not divisible by a.

2. The *geometric mean* of two non-negative numbers is the square root of their product. The *arithmetic mean* is half of their sum. An important fact is that the arithmetic mean is always at least as large as the geometric mean.

   (a) Turn the above English description into a precise mathematical claim, using formulas. Specifically, complete the following statement using formulas: "For all non-negative x and y, ..."

   (b) (8 points) Prove that this is true.

4. Induction

1. The sequence S_n is defined recursively for all $n \in \mathbb{N}$ as follows:

$$S_n = \begin{cases} S_{n-1} + S_{n-2} + 2S_{n-3} & \text{if } n \geq 3; \\ 3 - n & \text{if } n < 3. \end{cases}$$

   (a) This sequence satisfies $S_n \leq c2^n$ for some $c > 0$. What is the smallest integer c that works for all $n \in \mathbb{N}$?

   (b) (8 points) Prove that this bound holds.

   (c) What if we only wanted to bound S_n when $n \geq 4$. What is the smallest integer c that works in that case? (*Note: The sequence hasn't changed — we just don't care about S_i for $i \leq 3$ now.*)

2. (10 points) Prove using induction over the natural numbers that $11^n - 4^n$ is a multiple of 7, for all $n \in \mathbb{N}$. You should have a clear base case, induction hypothesis, and induction step.

5. Stable Matching

1. (3 points for each part – not 3 points per blank) Consider the following preferences lists for a stable matching instance for jobs *A*, *B*, and *C*, and candidates 1, 2, and 3.

Jobs	Preferences
A	3 > 1 > 2
B	2 > 3 > 1
C	3 > 2 > 1

Candidates	Preferences
1	B > C > A
2	C > A > B
3	A > C > B

   (a) What is the job optimal stable pairing for this instance?

   A: ☐ B: ☐ C: ☐

   (b) What is the candidate optimal stable pairing for this instance?

   A: ☐ B: ☐ C: ☐

   (c) Give another stable pairing for this instance that is neither job optimal nor candidate optimal, or indicate that there is none.

   ○ None OR A: ☐ B: ☐ C: ☐

2. If every job has a different candidate as their top choice, then there is a unique stable matching.

   ○ True ○ False

3. In a job optimal stable matching, some job always gets matched to its top candidate.

   ○ True ○ False

4. In a job optimal stable matching, a job can get matched to its least favorite candidate.

   ○ True ○ False

5. If a job is paired with its favorite candidate in a matching, that candidate can't be part of a rogue pair.

   ○ True ○ False

6. It's always possible to change the pairing produced by the propose and reject algorithm (with jobs proposing) by modifying the candidate preferences.

   ○ True ○ False

7. (6 points) Describe a stable matching instance (for any $n \geq 2$) in which the propose-and-reject algorithm matches every job to their top candidate, but every candidate gets their least favorite job.

6. Graphs

All graphs are simple unless otherwise specified.

1. (2 points each) For all of the questions the graph has 6 vertices, and for (a)-(g) you are to determine whether the statement is always true ("Yes"), always false ("No"), or if it depends on the specific graph ("Could be either").

   (a) A 6-vertex graph with 4 edges is connected.

   ◯ Yes ◯ No ◯ Could be either

   (b) A 6-vertex graph with 6 edges is connected.

   ◯ Yes ◯ No ◯ Could be either

   (c) A 6-vertex graph with 6 edges is acyclic.

   ◯ Yes ◯ No ◯ Could be either

   (d) A 6-vertex graph with 13 edges is connected.

   ◯ Yes ◯ No ◯ Could be either

   (e) A 6-vertex graph with 13 edges is planar.

   ◯ Yes ◯ No ◯ Could be either

   (f) What is the maximum number of edges in a 6-vertex graph?

2. In a graph with $|V|$ vertices, $|E|$ edges, and $|C|$ connected components, what is the minimum number of edges as a formula using $|V|$ and $|C|$?

3. The questions below deal with the graph K_7.

   (a) (2 points) K_7 has an Eulerian tour.

   ◯ True ◯ False

   (b) (2 points) Write a brief justification of your answer to part (a).

4. The questions below deal with the graph K_8.

   (a) (2 points) K_8 has an Eulerian tour.

   ◯ True ◯ False

   (b) (2 points) Write a brief justification of your answer to part (a).

5. If G is a connected 15 vertex graph, and has a planar embedding with 4 faces, how many edges does it have?

7. Graph Proofs

1. (6 points) Prove that if all vertices in a graph have odd degree, then the graph must have an even number of vertices.

2. (8 points) Consider the following procedure: given a tree $G = (V, E)$, with $|V| \geq 2$, and a designated "start vertex" $s \in V$, you start walking from vertex s, at each step choosing any untraversed edge incident to the current vertex (this is exactly the FINDTOUR(G, s) from the notes). Prove that you will get "stuck" (not be able to continue the walk) at a vertex $v \in V$ with degree 1.

8. Modular Arithmetic, FLT, CRT, and RSA

For questions that ask for a numerical answer mod m, always give a value in the range $0, \ldots, m-1$.

1. What is $5^{42} \bmod 41$?

2. What is the last digit of 519^{487}?

3. What is $43^{21} \bmod 55$?

4. Give any two specific values for a and m with $a \not\equiv 0 \pmod{m}$ such that $ax \equiv 0 \pmod{m}$ has a solution x with $x \not\equiv 0 \pmod{m}$.

5. If $k < x$, then $\gcd(x, x+k) = \gcd(x,k)$.

   ◯ True ◯ False

6. If $\gcd(a,m) = 1$ and $b \in \mathbb{Z}$, then $ax \equiv b \pmod{m}$ can have multiple solutions with $x \in \{0,1,\ldots,m-1\}$.

   ◯ True ◯ False

7. If $\gcd(a,m) = 2$ and $b \in \mathbb{Z}$, then $ax \equiv b \pmod{m}$ has either 0 or 2 solutions with $x \in \{0,1,\ldots,m-1\}$.

   ◯ True ◯ False

8. The following two parts refer to the RSA algorithm with $p = 11$ and $q = 7$, so $n = pq = 77$.

   (a) What is the smallest exponent e that would work with this modulus?

   (b) If we use $e = 29$, what is the corresponding d?

9. Modular Proofs

1. (6 points) Prove, using properties of modular arithmetic (*not induction*), that $11^n - 4^n$ is a multiple of 7 for all $n \in \mathbb{N}$.

2. (8 points) Let p be a prime, and let a be integer such that $a \not\equiv 0 \pmod{p}$ and $a^k \not\equiv 1 \pmod{p}$ for all $1 \leq k < p-1$. Show that for all $b \not\equiv 0 \pmod{p}$ there exists some non-negative $m < p-1$ such that $b \equiv a^m \pmod{p}$.

3. A value x is a "square root of 1 mod m" if $x^2 \equiv 1 \pmod{m}$. Such an x is a "*trivial* square root of 1" if $x \equiv 1 \pmod{m}$ or $x \equiv -1 \pmod{m}$, and it is *non-trivial* otherwise.

   (a) (6 points) Prove that for any modulus m, $(m-1)$ is a square root of 1.

   (b) $(m-1)$ is a non-trivial square root of $1 \pmod{m}$.

   ◯ True ◯ False

(c) (8 points) Prove that for prime modulus p, there are no non-trivial square roots of 1.

(d) Give a non-trivial square root of $1 \pmod{15}$.

10. Polynomials and Secret Sharing

1. $P(x)$ and $Q(x)$ are different polynomials over $GF(p)$. $P(x)$ has degree d_1 and $Q(x)$ has degree d_2, where $\max(d_1, d_2) < p$.

   (a) What is the maximum possible degree of $P(x) - Q(x)$?

   (b) What is the minimum possible degree of $P(x) - Q(x)$?

   (c) What is the maximum number of different x values for which $P(x) = Q(x)$?

   (d) What is the minimum number of different x values for which $P(x) = Q(x)$?

2. Alice, Bob, and Carol participate in a secret-sharing scheme in which any two of them can reconstruct the secret. They're using $GF(7)$.

   (a) What degree polynomial is used?

   (b) Alice and Bob are given shares $(1,6)$ and $(2,2)$. What is the secret?

   (c) If Carol has share $(3,y)$, what is y?

3. (6 points) When recovering the secret in Shamir's secret sharing scheme, the recovery algorithm must be executed somewhere. A group of k people with shares $(x_1, y_1), (x_2, y_2), \ldots, (x_k, y_k)$ decide to do it as follows: Everyone broadcasts their own share to the group, and then when everyone has received all k shares they can reconstruct the secret on their own. Person 1 wants to cheat, so that the recovered secret comes out to a value v that they select (for example, v may be the message "Person 1 gets a really big raise"). Person 1 delays broadcasting their own secret slightly, until after they see the other $k-1$ shares, and then they construct a fake share which they broadcast to everyone else.

   Describe what Person 1 would compute as their fake share, and justify that the reconstructed secret would be v.

11. Error Correcting Codes

1. Consider using the Berlekamp-Welch scheme to send an n-packet message, protected against errors in k packets.

   (a) How many packets do we send?

   (b) The message is encoded using polynomial $P(x)$ – what is the degree of $P(x)$?

   (c) What is the degree of the error locator polynomial $E(x)$ in the reconstruction algorithm?

   (d) If we only had $m < k$ errors, then how many roots does $E(x)$ have?

2. We transmit over a communication channel in which as many as 20% of the packets can be corrupted. Our message is n packets. Using Berlekamp-Welch error correction, how many packets do we need to send to ensure we can recover the message?

12. Counting Basics

For the questions in this section, you may leave your answer as an expression using factorial notation, $n!$, or the choose notation, $\binom{n}{k}$, unless otherwise specified.

1. Consider a 7 by 7 square grid. We start from the bottom left corner, and at each step choose to either go right or up. For example, we could go 4 steps right, 2 steps up, 3 steps right, then finally 5 steps up. How many possible paths are there to go from the bottom left corner to the top right corner?

2. Rummy is a card game that is played with a standard deck of 52 cards, and has hands of 7 cards. How many different Rummy hands are there?

3. How many different anagrams of the word ADDED are there? (An anagram is a rearrangement of the letters.)

4. How many anagrams of the word AARDVARK are there?

5. We roll a standard 6-sided die 10 times. How many different 10-roll sequences are there?

6. We roll a standard 6-sided die 10 times. An outcome is defined as the counts of how many times each value occurred. For example, "3 ones, 0 twos, 4 threes, 2 fours, 1 five, 0 sixes" could be an outcome. How many different outcomes are there?