

CS 70
Fall 2024

Discrete Mathematics and Probability Theory
Hug, Rao

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 258 points on this exam, with 15 total questions.

SID: _____

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. Warmup

(1 point) What is the conjunction of **all** student answers for this question?

True False

3. Propositional Logic

1. Consider the following statements, and determine whether they are *always true*, regardless of the values of the propositions P and Q .

If the statement is always true, answer “Yes”, and if the statement is not always true, answer “No”.

(a) $\neg\text{True}$

Yes No

(b) $P \vee [(P \implies Q) \wedge (P \implies \neg Q)]$

Yes No

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

Yes No

2. Consider the following implication, for a non-empty universe S :

$$[(\forall y \in S)(\exists x \in S)(Q(x) \wedge P(y))] \implies [((\exists x \in S)Q(x)) \wedge ((\forall y \in S)P(y))]$$

(a) Is the implication always true, regardless of the choice of predicates $P(\cdot)$ and $Q(\cdot)$?

Yes No

(b) Justify your answer, through either a counterexample or a brief explanation.

4. Proofs

1. (10 points) Let $n > 4$ be a composite number. Prove that

$$n \mid (n-1)!$$

Hint: Consider the cases when n is and is not a perfect square.

2. (6 points) Prove that for $r \in \mathbb{R}$, if r^2 is irrational, then r is irrational.

5. Induction.

(12 points) Prove that $7 \mid (3^{2n+1} + 2^{n-1})$ for $n \geq 1$ by induction. That is, you should have a clear base case, induction hypothesis, and induction step.

6. Stable Matchings.

1. Consider the following preference lists for jobs, A, B, C and candidates 1, 2, 3.

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

- (a) (3 points) Describe the job optimal pairing for this instance.

A: B: C:

- (b) (3 points) Describe the candidate optimal pairing for this instance.

A: B: C:

- (c) (3 points) Describe 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:

For the following parts, determine whether the statement is true or false.

2. If a job is paired with its least preferred candidate in the job optimal matching, then it is the least preferred job for every candidate.
 True False
3. If a job is paired with the same candidate in every stable matching, then that candidate is at the top of the job's preference list.
 True False
4. Recall that in a given day of the propose and reject algorithm with jobs proposing, candidates keep their best job offer on a string, and reject the rest. If a given candidate instead rejects all of their job offers on a given day (keeping none on a string), then the resulting matching (if there is one) will *always* be worse for this candidate.
 True False
5. If a job and candidate are paired in both the job optimal and candidate optimal matchings, then they are paired in every stable matching.
 True False

7. Graphs

All graphs are simple and undirected unless otherwise specified.

1. Consider a graph G with m edges and n vertices.

(a) If $m \geq n - 1$, then G must be connected.

True False

(b) If $m \leq n - 1$, then G must be acyclic.

True False

(c) If G is K_n , what is m in terms of n ?

(d) If G is a hypercube, what is m in terms of n ? (You may find $\log_2 n$ to be useful in your expression.)

(e) If an Eulerian tour exists in G , then m must be even.

True False

(f) What is the minimum number of connected components in G ? (Possibly in terms of m and/or n .)

(g) If G is acyclic and connected, then it must have at least _____ vertices of degree 1. (Give a tight bound, possibly in terms of m and/or n .)

(h) If G is acyclic and has c connected components, then what is m , possibly in terms of n and/or c ?

2. The number of odd degree vertices in a graph is always even.

True False

3. A d -dimensional hypercube can be edge colored with _____ colors. (Give a tight bound, possibly in terms of d .)

SID:

4. An odd-length cycle can be edge colored with _____ colors. (Give a tight bound.)

5. For a graph with $n + 1$ edges, there exists a vertex of degree at least _____. (Give a tight bound, possibly in terms of n . Your answer should be as large as possible and hold for every graph that meets the condition.)

8. Graph proofs.

All graphs are simple and undirected unless otherwise specified.

1. (8 points) Consider a simple connected planar graph with e edges and $v > 2$ vertices. Prove that if $e < 3v - 6$, then there is a face of size at least 4 (that is, there exists a face bounded by at least 4 edges). (Recall that in a simple planar graph, every face has size at least 3.)

2. (8 points) Consider a bipartite graph $G = (V, E)$ with an Eulerian Tour. Give a method to partition the edges of the graph into two graphs where every vertex has exactly half the degree, and justify your answer.

That is, form $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$, where $E_1 \cup E_2 = E$, $E_1 \cap E_2 = \emptyset$, and every vertex v has $d_1(v) = d_2(v) = d(v)/2$ where $d(v)$ is the degree of a vertex in G , and $d_i(v)$ is the degree of v in G_i .

9. Modular Proofs.

1. Consider the statement: For integers a, x, y , if $\gcd(x, y) = 1$ and $a \mid xy$, then $a \mid x$ or $a \mid y$.

(a) Indicate whether the statement is true or false.

True

False

(b) Justify your answer by providing a proof or a counterexample.

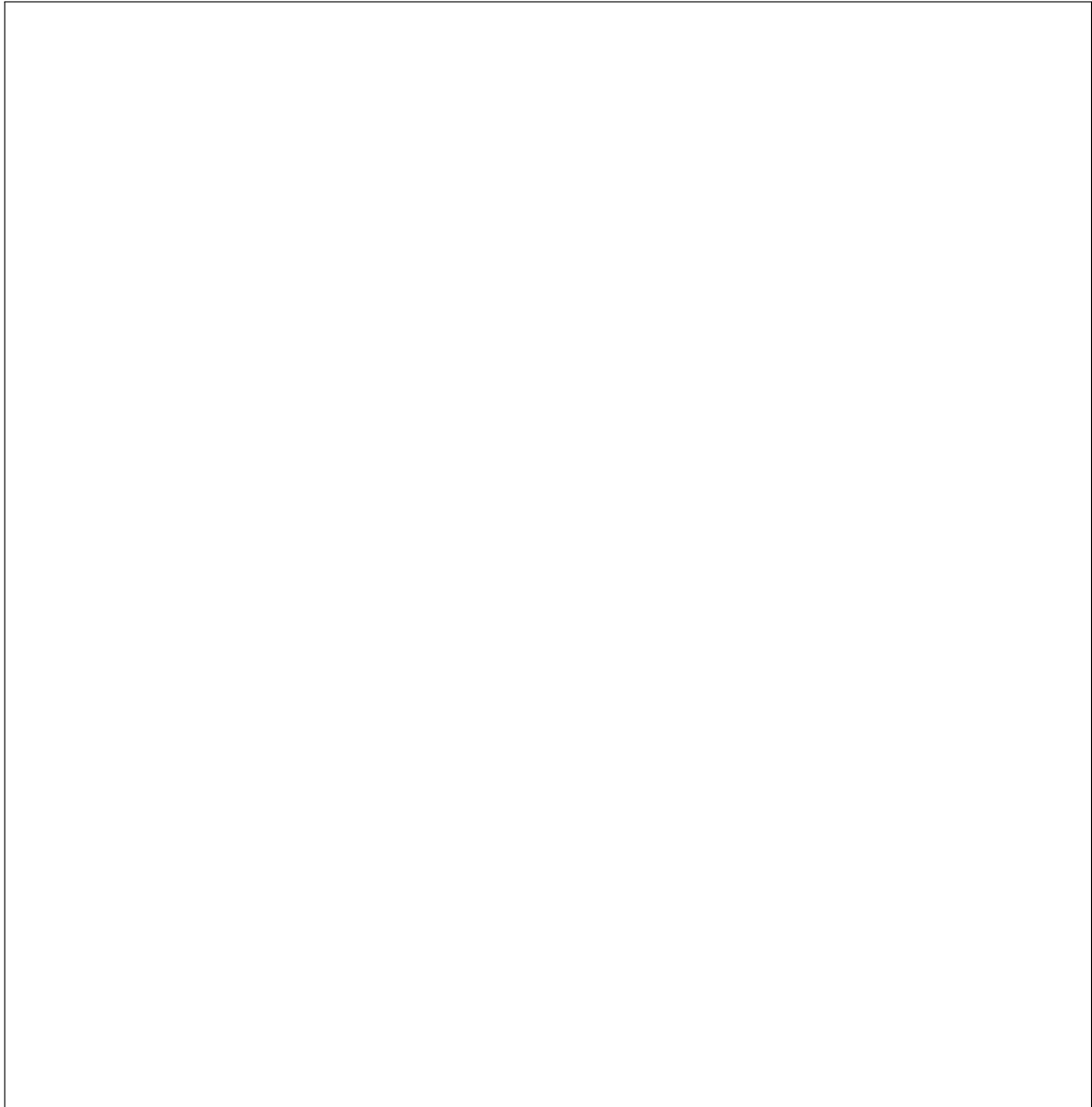
2. Consider $N = pqr$ for distinct primes p, q and r .

(a) What is the number of solutions to $qx \equiv 0 \pmod{N}$?

(b) What is $x^{(p-1)(q-1)(r-1)} \pmod{N}$, if $\gcd(x, N) = 1$?

SID:

- (c) (6 points) Use the Chinese Remainder Theorem and Fermat's Little Theorem to prove that your answer to the previous part is correct.



10. Modular: proof

Let a and n be positive integers. If m is the smallest positive integer such that $a^m \equiv 1 \pmod{n}$, we say that a has order m under arithmetic modulo n . In notation, we write that $\text{ord}_n(a) = m$.


1. What is the order of 3 under arithmetic modulo 5?

2. (6 points) Let $\text{gcd}(a, n) = 1$ and m be an integer. Prove that $a^m \equiv 1 \pmod{n}$ if and only if $\text{ord}_n(a) \mid m$.

3. (4 points) Prove that if p is a prime and a is an integer such that $p \nmid a$, then $\text{ord}_p(a) \mid p - 1$.

SID:

4. (8 points) Prove that there are no integers $n > 1$ where $n \mid (2^n - 1)$.



11. Modular arithmetic.

In the following parts, when working under arithmetic modulo N , give your answers in the range $\{0, 1, \dots, N - 1\}$.

1. What is $7^{26} \pmod{10}$?

2. What is the multiplicative inverse of 7 (mod 68)?

3. For integers $x \neq y$ and m, n with $\gcd(m, n) = d$, $x \equiv y \pmod{n}$ and $x \equiv y \pmod{m}$, then $|x - y| \geq$ _____.

4. How many solutions to the equation $10x \equiv 5 \pmod{505}$ are there for $x \in \{0, 1, \dots, 504\}$?

5. Consider an RSA scheme with public key (N, e) and private key d . Recall that the encoding of a message x is $E(x) = x^e \pmod{N}$ and that the decoding is $D(y) = y^d \pmod{N}$.

(a) $D(E(x)) \equiv E(D(x)) \pmod{N}$, for all x .

True False

(b) Give an expression that “decodes” a doubly encoded $y \equiv E(E(x)) \pmod{N}$. Express your answer in terms of y , possibly using $E(\cdot)$ and $D(\cdot)$.

(c) For $a \equiv x^e \pmod{N}$ and $b \equiv y^e \pmod{N}$, what is the value of $D(ab) \pmod{N}$? Your answer may be in terms of x and/or y .

12. Polynomials.

We say a polynomial is of degree d if it can be written in the form $a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$. We say that a polynomial is of degree exactly d if $a_d \neq 0$.

1. Give a polynomial of degree 2 under $\text{GF}(5)$ that contains the points $(0, 1)$, $(1, 0)$, and $(3, 0)$.

2. (3 points) Consider a polynomial of degree 2 under $\text{GF}(5)$ that contains the points $(0, 0)$, $(1, 1)$, and $(2, 4)$. In standard form, this polynomial can be written as $ax^2 + bx + c$. What are the coefficients of this polynomial?

$$a = \boxed{} \quad b = \boxed{} \quad c = \boxed{}$$

3. Given the points $(x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4)$, how many polynomials of degree at most 4 pass through these four points, when working in $\text{GF}(p)$, where $p \geq 5$ is prime? (Your answer may possibly be in terms of p .)

4. Given a polynomial $P(x)$ of degree exactly d and another polynomial $D(x)$ of degree exactly $d' < d$, we can perform polynomial division to construct polynomials $Q(x)$ and $R(x)$ such that $P(x) = Q(x)D(x) + R(x)$, where the degree of $R(x)$ is as small as possible.

- (a) What is the exact degree of $Q(x)$, possibly in terms of d and d' ?

- (b) Give a tight upper bound on the degree of $R(x)$, possibly in terms of d and d' .

13. Errors, erasures, and secrets.

1. Assume that 5 TA's have a point on a polynomial $P(x)$, and 3 professors have a point on a polynomial $Q(x)$, and there is a secret s , hidden at $P(0) = Q(0) = s$. A majority of either group should be able to reconstruct the secret. Also assume that we are working in arithmetic modulo p , where p is prime.

(a) What should the degree of the polynomial for $P(x)$ be?

(b) What should the degree of the polynomial for $Q(x)$ be?

(c) How large should the modulus p be? (Your answer may be in terms of s .)

2. Consider a polynomial $P(x) = 2x^2 + 3x + 3 \pmod{5}$, where we send $P(0), P(1), P(2), P(3)$ and $P(4)$ along a communication channel, and there was a corruption at $P(1)$.

(a) Recall that the error polynomial has the form: $E(x) = x + b_0 \pmod{5}$. What is $b_0 \pmod{5}$?

(b) Recall that $Q(x) = P(x)E(x) = q_dx^d + \dots + q_1x + q_0$.

i. What is d , the degree of $Q(x)$?

ii. What is q_d ?

iii. What is q_0 , in terms of b_0 ?

14. Polynomials, and Roots, and Counting

All polynomials below are over $\text{GF}(p)$. We say a polynomial is of degree d if it can be written in the form $a_d x^d + a_{d-1} x^{d-1} + \dots + a_0$. We say that a polynomial is of degree exactly d if $a_d \neq 0$.

In the following parts, you may leave your answers unsimplified (i.e. you can leave binomial coefficients, factorials, exponents, etc. as is), but you may not use any summation or product notation (i.e. you may not use \sum or \prod).

1. How many polynomials of degree exactly d over arithmetic modulo a prime p are there?

2. Any polynomial of degree exactly 1 has exactly 1 root.

True False

3. Give a quadratic polynomial with a root at $x = 1$ and nowhere else.

4. How many polynomials are there of the form: $a(x - r)^2$, where a is nonzero?

5. How many polynomials are there of the form: $a(x - r_1)(x - r_2)$ with $r_1 \neq r_2$, where a is nonzero? (Note that $(x - 1)(x - 2)$ is the same polynomial as $(x - 2)(x - 1)$.)

6. How many polynomials of degree exactly 2 have 0 roots?

7. Given k fixed constants r_1, \dots, r_k , how many polynomials are there of the form:

$$(x - r_1)^{b_1} (x - r_2)^{b_2} \dots (x - r_k)^{b_k}$$

$b_i \geq 1$ and $\sum_{i=1}^k b_i = d$, where $d \geq k$ is a given constant?

15. Counting.

Throughout this question, you may leave your answers unsimplified (i.e. you can leave binomial coefficients, factorials, exponents, etc. as is), but you should not use any summation or product notation (i.e. you may not use \sum or \prod).

1. A bridge game has 4 players who each get 13 cards, and each set of 13 cards is considered a bridge hand. Assume that we are working with a standard deck of cards, which has 52 cards in total.

(a) How many 13 card bridge hands are there? (The order of cards in a hand does not matter.)

(b) How many ways can the 52 cards be split among the four players? (That is, players 1 through 4 each get a different hand of 13 cards, and each card is in exactly one player's hand.)

2. How many solutions to $x_1 + \cdots + x_k = n$ are there, where each $x_i \geq -1$ and is an integer?

3. Consider the following sequence of letters: CANTSTANFURD

(a) How many ways can you rearrange the letters in CANTSTANFURD? (That is, how many anagrams are there?)

(b) Let x be the answer to part (a). How many orderings of the letters are there such that C is before S, and S is before D? Note that C, S, and D are not necessarily adjacent to each other. Express your answer in terms of x .

(c) Let x be the answer to part (a). How many orderings of the letters are there such that both A's are before the S? Note that the A's are not necessarily adjacent to the S or to each other. Express your answer in terms of x .

SID:

4. How many binary strings of length n are there with k ones?

5. How many ways are there to split five identical \$1 dollar bills among 4 head TA's?