
CS 70 Discrete Mathematics and Probability Theory Midterm
Fall 2026 Hug, Sabin

PRINT Your Name: _____

PRINT Your Student ID: _____

PRINT Your Exam Room: _____

PRINT the SID of the person to your left: _____

PRINT the SID of the person to your right: _____

PRINT the SID of the person in front of you: _____

PRINT the SID of the person behind you: _____

- 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.
- Anything written outside the boxes provided will not be graded.
- **Do not attempt to complete all of the questions on the midterm.** Plan out the topics you'd like to attempt on this exam and give yourself time to do the synthesis questions.
- You may use *one double-sided, handwritten, 8.5x11 cheat sheet*. 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.**
- If you've already passed a topic, there is no benefit to re-attempting that topic's question.

Topics on This Midterm

☐ Direct Proofs 2	☐ Modular Arithmetic 8	☐ Secret Sharing & ECCs . . . 14
☐ Propositional Logic 4	☐ CRT 9	☐ Graphs 17
☐ Proof Techniques 5	☐ RSA 10	☐ Graph Induction 18
☐ Induction 7	☐ Polynomials 12	☐ Stable Matching 19

Additionally, **there are two synthesis questions on pg. 20 and pg. 21.**

SID:

Direct Proofs

Pass Threshold: There are 3 questions for this topic. To pass the topic on this midterm, you must get at least 2 questions correct.

Prove each of the following claims with a direct proof.

- (a) For every natural number n , if n is odd then $3n + 4$ is odd.

- (b) For any $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$, then $a \mid c$.

SID:

(c) For all $n \in \mathbb{N}$, if n is divisible by 3, then $(n+1)^2 + 2$ is divisible by 3.

Propositional Logic

Pass Threshold: There are 6 questions for this topic. To pass the topic on this midterm, you must get at least 4 questions correct.

(a) Define:

$S(x)$: student x studies regularly for the CS 70 final exam

$P(x)$: student x passes the exam

Translate the following statement into predicate logic: Not every student who studies regularly for the CS 70 final exam passes it.

(b) Suppose that P is true, Q is false, and R is true. Determine whether the following proposition is true or false.

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

☐ True ☐ False

Determine whether the following proposition is Always True, Always False, or could be Either:

(c)

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

☐ Always True ☐ Always False ☐ Either

(d) Let $P(x)$ and $Q(x)$ be predicates over a universe with at least two elements.

$$(\forall x (P(x) \implies Q(x))) \vee (\forall x (Q(x) \implies P(x))).$$

☐ Always True ☐ Always False ☐ Either

Determine whether the following propositions are logically equivalent:

(e)

$$\neg(P \wedge Q) \vee R \quad \text{and} \quad (R \wedge \neg Q) \vee P$$

☐ Logically Equivalent ☐ Not Logically Equivalent

(f)

$$\exists x (P(x) \wedge \neg Q(x)) \quad \text{and} \quad \neg \forall x (P(x) \implies Q(x))$$

☐ Logically Equivalent ☐ Not Logically Equivalent

SID:

Proof Techniques

Pass Threshold: There are 2 questions for this topic. To pass the topic on this midterm, you must get at least 2 questions correct.

- (a) Prove that there is a unique real number x that satisfies

$$x + a = a + x = a$$

for all $a \in \mathbb{R}$.

SID:

- (b) Prove the following statement: for any integers a and b , a is even and b is odd if and only if $ab + 7b - 2a - 14$ is odd.

Induction

Pass Threshold: There is 1 question for this topic. To pass the topic on this midterm, you must get at least 1 question correct.

- (a) Alice and Zoe play a game with two piles of raisins, taking turns. On her turn, a player must perform two actions:
1. Choose one pile and completely eat all its raisins.
 2. From the remaining pile, pick *any positive number* of raisins to gather into a *new* second pile, preparing the next turn. But if the remaining pile has only 1 raisin, then the player cannot split the pile and instead **loses the game**.

Alice gets the first turn. Prove that if there is a pile containing an even number of raisins on Alice's turn, then Alice can guarantee she wins. (*Hint.* Use induction the size of the even pile **on Alice's turns**. Trusting the claim, Alice wants to always receive an even pile on **her** next turn, but how can she force this from Zoe?)

SID:

Modular Arithmetic

Pass Threshold: There are 5 questions for this topic. To pass the topic on this midterm, you must get at least 4 questions correct.

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

(a) Compute $67^{6767} \pmod{68}$.

(b) Compute $98 \cdot 99 \cdot 100 \pmod{101}$.

(c) Let $x \equiv 5 \pmod{12}$. Find k such that $2x + 6 \equiv k \pmod{6}$.

(d) Prove that if $a \equiv b \pmod{m}$, then $a + c \equiv b + c \pmod{m}$ for any integer c .

(e) For how many values of $a \in \{0, 1, \dots, 15\}$ does a^{-1} exist modulo 16?

SID:

CRT

Pass Threshold: There is 1 question for this topic. To pass the topic on this midterm, you must get at least 1 question correct.

- (a) Find the smallest natural number x that satisfies all three of the following congruences:

$$x \equiv 2 \pmod{5}$$

$$x \equiv 1 \pmod{6}$$

$$x \equiv 4 \pmod{7}$$

SID:

RSA

Pass Threshold: There are 3 questions for this topic. To pass the topic on this midterm, you must get at least 2 questions correct.

Each subpart should be able to be done independently of the other subparts.

- (a) Alice and Bob set up an RSA scheme where Alice chooses $p = 17$, $q = 5$, and $e = 23$. What is Alice's public key, and what encryption function $E(x)$ does Bob use to send her a message x ? Box your answers to both questions; both must be correct to receive credit.

- (b) Alice and Bob set up an RSA scheme where $p = 17$, $q = 5$, and $e = 23$. Find the smallest positive value of d that can serve as the private key.

SID:

- (c) Alice sets up RSA with $p = 7$, $q = 13$, $e = 5$, and $d = 29$. Worried that her scheme is insecure, she changes e to 77 and keeps everything else the same. Is the scheme still correct? Briefly explain in 3 sentences or less.

Polynomials

Pass Threshold: There are 3 questions for this topic. To pass the topic on this midterm, you must get at least 3 questions correct.

- (a) Use Lagrange interpolation to find the unique polynomial $p(x)$ of degree at most 2 over $\text{GF}(11)$ that passes through all of the following points:

$$(1, 7) \quad (3, 5) \quad (4, 0)$$

Make sure $p(x)$ is of the form $a_2x^2 + a_1x^1 + a_0$, where $a_2, a_1, a_0 \in \{0, 1, \dots, 10\}$. To help you get started, we've provided $\Delta_2(x)$, which corresponds to the second point given.

$$\Delta_2(x) = 5x^2 + 8x + 9$$



SID:

- (b) Let $f(x)$ and $g(x)$ be polynomials over $\text{GF}(11)$ of degrees exactly 4 and 3, respectively. What is the greatest possible number of distinct roots of $f(x)g(x)$?

- (c) Find a polynomial with degree strictly less than 13 that is equivalent to $f(x) = 70x^{72} + 2x^{26} + 7$ over $\text{GF}(13)$.

Secret Sharing & ECCs

Pass Threshold: There are 4 questions for this topic. To pass the topic on this midterm, you must get at least 3 questions correct.

- (a) Sidharth wants to send you a message with an unknown number of points. To guard against 1 general error, Sidharth sends you 5 points. How many points were in the original message that Sidharth wanted to send?

- (b) Professor Sabin is sending Ricardo an n -packet email. The email service that Professor Sabin uses takes k packets and replaces them with random values.

True or False: Ricardo will be able to recover the message using the Berlekamp–Welch algorithm if Professor Sabin sends $n + k$ packets.

☐ True ☐ False

- (c) Large Technology @ Berkeley recently acquired a huge sponsorship from Computing Co! To protect the sum of money, they secure it with a polynomial secret sharing scheme involving 2 co-presidents and 10 officers. To access the funds, they require either 2 co-presidents to contribute their secrets, or 1 co-president and 7 officers. If no co-presidents are involved, it should be impossible to access the funds.

Design a secret sharing scheme for this, using polynomials of lowest degree possible.

To get full credit for this question, you must get all subparts correct.

- (i) How many polynomials do you need for this system to work?

- (ii) What are the degrees of your polynomials? *You do not need to fill in every box.*

Polynomial 1

Polynomial 2

Polynomial 3

Polynomial 4

Polynomial 5

Polynomial 6

Polynomial 7

Polynomial 8

- (iii) How many points does each co-president get?

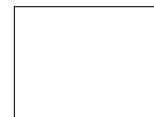
- (iv) How many points does each officer get?

- (d) The answer to this question, s , is locked in a degree-1 polynomial $P(x)$ over $\text{GF}(p)$ with $p = 5$, where $P(0) = s$. However, in a series of (un)fortunate events, 3 of the points on $P(x)$ have been leaked on this midterm.

$P(1)$ = The page number of the front page $\pmod{p}$

$P(2)$ = The page number of the Induction question $\pmod{p}$

$P(3)$ = The page number of the Modular Arithmetic question $\pmod{p}$



Graphs

Pass Threshold: There are 5 questions for this topic. To pass the topic on this midterm, you must get at least 4 questions correct.

(a) K_4 is planar.

☐ True ☐ False

(b) K_5 has an Eulerian tour.

☐ True ☐ False

(c) All dice can be viewed as planar graphs wrapped around a sphere. A 12-sided die thus has 12 faces to roll. If we know there are 20 pointy vertices to 12-sided dice, then how many edges are there on a 12-sided die?

(d) In a 5-dimensional hypercube (i.e. the vertices are all 5-bit strings where two vertices share an edge if they differ in exactly one bit location), what is the length of the shortest path from the vertex labelled 10010 to the vertex labelled by 01000?

(e) Prove that if a graph has a vertex that has odd degree, there must be another vertex that has odd degree.

Graph Induction

Pass Threshold: There is 1 question for this topic. To pass the topic on this midterm, you must get at least 1 question correct.

- (a) For a graph $G = (V, E)$, we know the Degree-Sum Formula (a.k.a. The Handshake Lemma):

$$\sum_{v \in V} \deg(v) = 2|E|$$

We've argued intuitively that this is true because each edge is double-counted. Use induction to prove that the degree-sum formula holds for all undirected graphs.

Stable Matching

Pass Threshold: There are 5 questions for this topic. To pass the topic on this midterm, you must get at least 3 questions correct.

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

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

- (a) Consider the following pairing: $(A, 1)$, $(B, 2)$, and $(C, 3)$. Is this matching stable?

☐ Yes ☐ No

If you answered *No*, name a rogue couple.

- (b) Describe a stable matching between jobs and candidates from these preferences (if the previous question's pairing was stable, then list a different matching that is also stable).

A : B : C :

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

- (c) It is impossible for a pairing to be stable if the pairing has a couple (J, C) such that C is J 's least favorite candidate and J is C 's least favorite job.
- ☐ True ☐ False
- (d) 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
- (e) In a stable matching instance, if we run the propose-reject algorithm twice, once with jobs proposing and once with candidates proposing and the exact same pairing is produced by both runs, what can we say about the number of stable matchings?
- ☐ None ☐ Exactly one ☐ Must be more than one ☐ Not determined by this outcome

Synthesis Question: CRT, revisited...

Consider the following congruences:

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

$$x \equiv b \pmod{q}$$

where p, q are coprime. Recall that the Chinese Remainder Theorem tells us that there exists a unique solution $x \pmod{pq}$.

Now, consider the new system of congruences:

$$cx \equiv ca \pmod{cp}$$

$$dx \equiv db \pmod{dq}$$

Where c, d are nonzero natural numbers. How many solutions x in mod $cdpq$ exist (if any)?

Justify your answer.

Synthesis Question: Rogue Delegates

The planning committee for The International Conference on Hackathon Organization has designed the following secret sharing scheme:

70 points of a 49-degree shared polynomial have each been assigned to the 70 delegations, one point per delegation.

Each delegation contains 10 delegates. They each receive a point of a degree 5 delegation-specific polynomial. Delegates can come together to recover their delegation's point on the shared polynomial using the delegation-specific polynomial.

A *rogue delegate* is an all-powerful delegate: they know all of the polynomials and have control over which delegation that they are placed in. The rogue delegates purposely manipulate their point on their delegation-specific polynomial to mess up the conference.

The planning committee will use the Berlekamp-Welch algorithm on the delegation-specific polynomials and on the shared polynomial to attempt to recover the correct secret. What is the smallest number of rogue delegates that can attend the conference and corrupt the committee's ability to recover the correct secret?

Justify your answer.

SID:

Doodle Page.

Feel free to use this page for scratch work, providing any comments about the exam, or to draw a fun picture!