CS 70 Discrete Mathematics and Probability Theory
Fall 2023 Rao and Tal

# Midterm

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

PRINT Your Student ID: _____

PRINT Your Exam Room: _____

SID of person to left: _____ SID of person to right: _____

SID of person in front: _____ SID of person in back: _____

**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.**
- 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 228 points on this exam, with 15 total questions.

**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 instructor and GSI, 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 greatest common divisor of **all** finite natural number student answers to this question?

## 3. Propositional Logic (and other stuff.)

1. Let $P$, $Q$ and $R$ be propositions.
   (a) $P \implies Q$ is equivalent to $\neg P \implies \neg Q$.

   ◯ True ◯ False

   (b) $(P \wedge Q) \implies R$ is equivalent to $\neg R \implies$ _____.

2. For predicates $P(x)$ and $Q(x)$,

$$\neg(\exists x \in \mathbb{Z})(P(x) \vee Q(x)) \equiv (\forall x \in \mathbb{Z})(\neg P(x) \wedge \neg Q(x)).$$

   ◯ True ◯ False

3. For predicates $P(x)$ and $Q(x,y)$,

$$\neg(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(P(x) \wedge Q(x,y)) \equiv (\exists x \in \mathbb{N})(\forall y \in \mathbb{N})(\neg P(x) \wedge \neg Q(x,y)).$$

   ◯ True ◯ False

4. $(\forall a,b \in \mathbb{N})(\frac{a}{b} \neq \sqrt{2})$.

   ◯ True ◯ False

5. $(\forall n \in \mathbb{N})\left[(\exists i \in \mathbb{N})(i^2 = n) \vee (\forall a,b \in \mathbb{N})(\frac{a}{b} \neq \sqrt{n})\right]$.

   ◯ True ◯ False

**4. Short proofs.**

First, say whether each statement is true or false, and then prove or give a counterexample. The proof or counterexample should be brief.

1. (5 points) If $a \mid b$ and $a \mid c$, then $a \mid (b+5c)$.

◯ True ◯ False

2. (5 points) If $b^2 = n$, then $n \mid b$.

◯ True ◯ False

3. (5 points) If $n$ is not a perfect square, and its prime factorization is $p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$, then at least one $k_i$ must be odd.

◯ True ◯ False

**5. Long proofs.**

1. (6 points) Consider the recursive sequence defined by

$$x_1 = 1 \text{ and } x_n = \sqrt{1 + x_{n-1}} \text{ for all } n \geq 2.$$

Prove that $x_n < 2$ for all $n \geq 1$.

2. (10 points) Prove that $2^{n+2} + 3^{2n+1}$ is divisible by 7 for all $n \geq 1$.

**6. Stability in Matchings.**

We consider instances of the stable matching problem below.

1. In an instance, if a job and candidate are paired in both the job propose and candidate propose matching algorithms, they are partners in all stable pairings.

   ◯ True ◯ False

2. In an instance, if some job and candidate are paired in both the job and candidate optimal pairings, then there is only one possible stable pairing for this instance.

   ◯ True ◯ False

3. For an $n = 2$ instance, a stable pairing is always job optimal or candidate optimal (or both).

   ◯ True ◯ False

4. There are instances where a candidate can reject the wrong job and do better (i.e. end up with a more preferable partner).

   ◯ True ◯ False

## 7. Graphs

You may assume all graphs in this section are simple (as defined in the notes) unless otherwise specified. Also a graph can't have zero vertices.

1. A hypercube of dimension $n$ has an even number of edges for $n \geq$ ____. (Give a tight bound.)

2. A complete graph, $K_n$, has an even number of edges for any $n > 3$.

   ◯ True ◯ False

3. Recall a cut in a graph $G = (V, E)$ is a subset $S \subseteq V$. We define the *edges in the cut* $S$ to be the edges with one endpoint in $S$ and the other endpoint in $V \setminus S$.

   (a) In a complete graph on $n$ vertices, given a cut of size $k$, how many edges are in this cut?

   (b) For an $n$-vertex tree, what is the least number of edges in any cut? (Note $|S| \geq 1$ and $|V \setminus S| \geq 1$.)

   (c) For an $n$-vertex tree, what is the maximum number of edges in any cut?

4. Adding an edge $e$ to a graph either reduces the number of connected components or creates (at least) one cycle that uses edge $e$.

   ◯ True ◯ False

5. What is the minimum number of connected components for any graph with $n$ vertices and $e$ edges?

6. An $n$ vertex graph with ___ edges must have a cycle. (Recall graphs are simple unless otherwise stated. Give a tight bound.)

## 8. Graph: proofs

1. Recall that an edge coloring of a graph $G = (V, E)$ is a coloring of edges such that no pair of edges sharing a common vertex have the same color.

   (a) A dimension $n$ hypercube can be edge colored with $n$ colors.

   ◯ True ◯ False

   (b) Any graph with maximum degree $d$ can be edge colored with $d$ colors.

   ◯ True ◯ False

   (c) Any bipartite graph can be edge colored with 2 colors.

   ◯ True ◯ False

   (d) Consider an $n > 2$ vertex bipartite graph where every vertex has degree $d$, and where the edges can be decomposed into Hamiltonian cycles. That is, there is a set $S$ of Hamiltonian cycles in $G$ where each edge appears in exactly one Hamiltonian cycle. Recall a Hamiltonian cycle is a simple cycle in the graph that contains every vertex.

      i. What is the number of edges in this graph?

      ii. How many Hamiltonian cycles are in $S$?

      iii. (5 points) Prove that any such graph can be edge colored with $d$ colors.

2. (6 points) Recall a bipartite graph $G = (L, R, E)$ has vertices $V = L \cup R$, and edges $(u, v) \in E$ such that $u \in L$ and $v \in R$.

   A *Hall set* is a set $S \subseteq L$, where $|N(S)| < |S|$, and $N(S)$ is the set of neighbors of vertices in $S$. That is,

   $$N(S) = \{v \mid (\exists u \in S)((u, v) \in E)\}.$$

   Argue that if every vertex has degree exactly $d > 0$, there is no Hall Set. (Hint: think about the sum of the degrees in $S$.)

**9. Modular Arithmetic.**

1. What is $7^{50} \pmod{35}$?

2. Suppose $q$ is prime and $N = q^2$.
   (a) How many elements in the set $S = \{0, 1, \ldots, N-1\}$ are relatively prime to $N$?
   (b) If $a$ has $\gcd(q, a) = 1$, then $a$ has an inverse modulo $N$.
   ◯ True ◯ False
   (c) $a^x \equiv a \pmod{N}$ for $x = 1$ or $x =$ _____ if $gcd(a, N) = 1$. (Answer is an expression possibly involving $N, q$ or $S$. Hint: what is the function $f(x) = ax \pmod{N}$ on the set $S$?)

3. If $ab \equiv 0 \pmod{n}$ then either $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$.
   ◯ True ◯ False

4. An integer $a$ is an integer linear combination of $x$ and $y$ if $a = ix + jy$ for some integers $i, j$.
   Consider two linear combinations of $x$ and $y$: $m = ax + by$ and $n = cx + dy$.
   (a) Any integer linear combination of $m$ and $n$ is an integer linear combination of $x$ and $y$.
   ◯ True ◯ False
   (b) The smallest positive number that is an integer linear combination of $x$ and $y$ is $\min(x, y)$.
   ◯ True ◯ False
   (c) The smallest positive number that is an integer linear combination of $x$ and $y$ is $\gcd(x, y)$.
   ◯ True ◯ False

5. If $x \equiv a \pmod{m}$ and $x \equiv a \pmod{n}$, where $\gcd(n, m) = 1$, then $x \equiv a \pmod{mn}$.
   ◯ True ◯ False

6. Consider an integer $x$ such that $x \equiv a \pmod{m}$ and $x = a + kn$ for integers $k$ and $n$, where $\gcd(m,n) = q$.

   (a) If $x$ is non-zero, what is the smallest *strictly positive* value for $k$ where $x$ satisfies the properties?

   (b) How many values of $x \in \{0, \ldots, mn-1\}$ are solutions?

**10. Modular Arithmetic: generator?**

Consider a prime $p > 2$ such that $(p-1) = q_1 \cdot q_2 \cdots q_k$ for distinct primes $q_1, \ldots, q_k$.

1. (3 points) Prove that there is a nonzero element $x$ such that $x^n - 1 \not\equiv 0 \pmod{p}$, where $n < p-1$.

2. (6 points) Prove that there is a nonzero element $a \not\equiv 1 \pmod{p}$ such that $a^{q_i} \equiv 1 \pmod{p}$ for any $i \in \{1, \ldots, k\}$.

3. (6 points) Let the *order* of $x$ be the smallest positive integer $k$ such that $x^k \equiv 1 \pmod{p}$. Prove that if $x^q \equiv 1 \pmod{p}$ and $d$ is the order of $x$, then $d \mid q$.

**11. Swiper, no swiping!**

(6 points) Suppose Dora and Boots are exchanging a message via RSA with $N = 15$ (where $p = 3$ and $q = 5$). Swiper spies the encrypted message $E(x) \equiv 10 \pmod{15}$. If the original message $x$ is less than 15, explain how Swiper can recover $x$ and provide an explicit value for $x$ without knowing the encryption key $e$.

**12. Polynomial and Applications.**

1. If a secret is encoded at $x = 0$ into a line that goes through the points $(1,1)$ and $(2,3)$ in arithmetic modulo 5, then what is the secret? (Answer should be in $\{0,\ldots,4\}$.)

2. Consider two polynomials $P(x)$ and $Q(x)$, both with degrees exactly $d_P$ and $d_Q$, respectively.
   (a) What is the degree of $P(x)Q(x)$?
   (b) Suppose we perform polynomial division to compute $P(x)/Q(x)$, resulting in the equation $P(x) = D(x)Q(x) + R(x)$ for some other polynomials $D(x)$ and $R(x)$.
      i. What is the degree of $D(x)$, possibly in terms of $d_P$ and $d_Q$?
      ii. What is the maximum degree of $R(x)$, possibly in terms of $d_P$ and $d_Q$?
      iii. If $R(x) = 0$, then all the roots of $Q(x)$ are roots of $P(x)$.
      ◯ True ◯ False
      iv. If $R(x) = 0$, then all the roots of $D(x)$ are roots of $P(x)$.
      ◯ True ◯ False

3. Suppose we want to send a message of size 1, protecting against 1 general error, where the received packets are $R(1) = 2$, $R(2) = 1$, $R(3) = 2$ working modulo 5. Consider the Berlekamp–Welch scheme in the following.
   (a) What is the error polynomial $E(x)$?
   (b) What is $Q(x)$?

## 13. Blank Space[s]

1. (1 point each) We will walk through a proof for the following identity:

$$\sum_{i=0}^{n} \binom{n}{i} \sum_{j=0}^{n-i} \binom{n-i}{j} = 3^n.$$

Fill in the blanks below.

Suppose we have three bins labeled $A$, $B$, and $C$, and $n$ balls labeled 1 through $n$.

On the RHS, we go one ball at a time. Each ball can go into 3 possible bins, so the total number of ways to distribute the $n$ balls is __(a)__.

On the LHS, we go one bin at a time. From the $n$ balls we start with, there are __(b)__ ways to put some arbitrary number of __(c)__ balls into bin $A$. Then, from the remaining __(d)__ balls, there are __(e)__ ways to put some arbitrary number of __(f)__ balls into bin $B$. Then, we put all the remaining __(g)__ balls into bin $C$, which happens in __(h)__ way(s).

(a)

(b)

(c)

(d)

(e)

(f)

(g)

(h)

2. (1 point each) The password to unlock the CS70 Fall 2023 Midterm Solutions document can be opened with a secret code. The solutions should only be released when **both of these two conditions** are met.

   - Condition 1: Either all 14 TAs must agree, OR 10 TAs and Alec Li must agree
   - Condition 2: 20 Readers must agree

   Fill in the blanks to complete the following secret sharing scheme that satisfies these conditions.

   Because there are 2 conditions, we encode the secret code to the solutions document as $P(0)$ in a degree __(a)__ polynomial $P(x)$.

   We will encode 1 point from $P(x)$ as the secret to another polynomial $Q(x)$ corresponding to Condition 1. $Q(x)$ will have degree __(b)__, and __(c)__ point(s) will given to each TA. Alec Li specifically will receive __(d)__ point(s). All points given are distinct.

   To satisfy Condition 2, we encode another point from $P(x)$ as the secret to another polynomial $R(x)$. $R(x)$ will be a degree __(e)__ polynomial and each Reader will be given __(f)__ point(s).

(a)

(b)

(c)

(d)

(e)

(f)

**14. Two dice or not two dice**

Shreyas is rolling a fair six-sided die 3 times. He writes down the resulting three numbers as a sequence. One possible sequence is 4,2,1. You may leave your answer in terms of exponents and binomial coefficients without simplifying.

1. Compute the total number of possible outcomes for the sequence.

2. Compute the total number of sequences such that the rolls are strictly increasing.

3. Compute the total number of sequences such that the rolls are nondecreasing.

4. Compute the total number of ways such that 1 does not appear in any of the rolls.

5. Compute the total number of sequences where at least one of the first two rolls is the number 1.

6. Compute the total number of sequences where the product of all the rolls is even.

**15. Proof: Countability**

(6 points) Prove that the set of irrational numbers ($\mathbb{R} \setminus \mathbb{Q}$) is uncountable.