CS 70 Discrete Mathematics and Probability Theory
Summer 2025 Tate

Midterm Solutions

PRINT Your Name: Oski Bear

SIGN Your Name: *OSKI*

Do not turn this page until your instructor tells you to do so.

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) $(P \wedge \neg P) \implies Q$
   Answer: True. $P \wedge \neg P$ is always false (a contradiction), so the implication is vacuously true (Note 1, Section 1).
   (b) $P \implies (Q \vee \neg Q)$
   Answer: True. The conclusion, $Q \vee \neg Q$ is always true, which means the implication is always true (called "trivially true" – Lecture 1).
   (c) $(P \vee \neg P) \implies (Q \wedge \neg Q)$
   Answer: False. In this one, the hypothesis is always true, and the conclusion is always false, giving "true $\implies$ false" which is false.
   (d) $(P \vee Q) \implies (P \wedge Q)$
   Answer: Could be either. If P is true and Q is false, we have "true $\implies$ false" (which is false), but if both P and Q are true we have "true $\implies$ true" which is true.
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 $\forall x \exists y[P(x) \implies Q(x,y)]$
   Answer: Equivalent. You can always move a quantifier to the left, over basic logic that doesn't have a different binding for the quantified variable (but not other quantifiers), and have an equivalent statement.
   (b) $\exists x[P(x) \implies \forall y\, R(x,y)]$ and $\forall x[P(x) \vee \exists y\, R(x,y)]$
   Answer: Not equivalent. An example illustrates this: Consider a $P(x)$ and $R(x,y)$ which are false for all values of x and y. In this case, the implication in the first statement is vacuously true for all x, so the proposition is true. However, for the second proposition, since $R(x,y)$ is always false then $\exists y\, R(x,y)$ is false for all x as is $P(x)$, so the second proposition is false.

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:

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

Answer: $\exists x\, R(x) \vee \forall x \exists y S(x,y)$
Explanation: We first apply De Morgans Law to the AND, giving $\neg\forall x\, P(x) \vee \neg\exists x \forall y Q(x,y)$, and then applying De Morgans Law for quantifiers to get $\exists x\, \neg P(x) \vee \forall x \exists y \neg Q(x,y)$. Finally, substituting for the negated propositions gives the answer.

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.
Answer: This is easy to prove by contraposition. The contrapositive is "if both b and c are divisible by a, then $2b+3c$ is divisible by a. If b and c are divisible by a, then there exist integers k_1 and k_2 such that $b = k_1 a$ and $c = k_2 b$, so $2b+3c = 2k_1 a + 3k_2 a = (2k_1+3k_2)a$. Therefore $2b+3c$ is a multiple of 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, ..."
   Answer: The full statement is: For all non-negative x and y, $\frac{x+y}{2} \geq \sqrt{xy}$.
   (b) (8 points) Prove that this is true.
   Answer: Assume for the sake of contradiction that there are non-negative x and y such that $\frac{x+y}{2} < \sqrt{xy}$. If we multiply both sides by 2 and then square them, we get

$$(x+y)^2 < 4xy \implies x^2+2xy+y^2 < 4xy \implies x^2-2xy+y^2 < 0 \implies (x-y)^2 < 0.$$

   A squared value cannot be less than zero, so we reach a contradiction.

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 $n \in \mathbb{N}$?
   Answer: 3. Thinking through how the following proof works gives this value: any value of c works in induction step, if it works for the first 3 values. Looking at $S_0 = 3$, $S_1 = 2$, and $S_2 = 1$ shows that the smallest c that works for $n \geq 0$ is $c = 3$ (constrained by S_0).

(b) (8 points) Prove that this bound holds.
Answer: By strong induction on n.
Base case: We verify three values directly in the base case:
$S_0 = 3$, which is $\leq 3 \cdot 2^0 = 3$.
$S_1 = 2$, which is $\leq 3 \cdot 2^1 = 6$.
$S_2 = 1$, which is $\leq 3 \cdot 2^2 = 12$.

In the following, we use the generic constant c, and everything works for *any* $c > 0$.
Induction hypothesis: Assume that for all $n \leq k$, $S_n \leq c \cdot 2^n$.
Induction step: We prove that for $n = k+1$, $S_{k+1} \leq c \cdot 2^{k+1}$.
Using the definition and the induction hypothesis, we get

$$\begin{aligned} S_{k+1} &= S_k + S_{k-1} + 2S_{k-2} \\ &\leq c \cdot 2^k + c \cdot 2^{k-1} + 2 \cdot c \cdot 2^{k-2} \\ &= \frac{1}{2} c 2^{k+1} + \frac{1}{4} c 2^{k+1} + \frac{2}{8} c 2^{k+1} \\ &= c 2^{k+1}. \end{aligned}$$

This completes the induction step and the proof.

(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.*)
Answer: 1. Using the reasoning in part (a) and the insight from the proof, we only need a c that works for S_4, S_5, and S_6. These three give the following constraints for c:

$$S_4 = 9 \implies c \geq \frac{9}{2^4} = \frac{9}{16}$$

$$S_5 = 14 \implies c \geq \frac{14}{2^5} = \frac{7}{16}$$

$$S_6 = 25 \implies c \geq \frac{25}{2^6} = \frac{25}{64}$$

In all cases, $c = 1$ works, so $c = 1$ is the smallest integer that works in the bound.

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.
Answer: We prove that for all $n \in \mathbb{N}$, there is an integer m such that $11^n - 4^n = 7m$.
Base case $(n = 0)$*:* When $n = 0$, $11^n - 4^n = 1 - 1 = 0$, which is $7 \cdot 0$.
Induction hypothesis: Assume that for $n = k$, there is an integer m such that $11^k - 4^k = 7m$.
Induction step: We prove that for $n = k+1$, there is an integer m' such that $11^{k+1} - 4^{k+1} = 7m'$.
We simplify

$$11^{k+1} - 4^{k+1} = 11 \cdot 11^k - 4 \cdot 4^k = 7 \cdot 11^k + 4 \cdot 11^k - 4 \cdot 4^k = 7 \cdot 11^k + 4(11^k - 4^k).$$

The final part, in parentheses, can be replaced by $7m$ by the induction hypothesis, giving

$$11^{k+1} - 4^{k+1} = 7 \cdot 11^k + 4 \cdot 7m = 7(11^k + 4m).$$

Therefore, $11^{k+1} - 4^{k+1}$ is a multiple of 7, which completes the induction step and proof.

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?

   Answer: A:3; B:1; C:2.
   Running the propose-and-reject algorithm gives the job-optimal matching.

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

   Answer: A:3; B:1; C:2.
   Running the propose-and-reject algorithm with candidates proposing gives the candidate-optimal matching.

   (c) Give another stable pairing for this instance that is neither job optimal nor candidate optimal, or indicate that there is none.
   Answer: None.
   Since the job optimal and candidate optimal matching are the same, there are no other stable matchings.

2. If every job has a different candidate as their top choice, then there is a unique stable matching.
   Answer: False. Consider a case where every candidate also has a different job as their top choice, but none of which agree with the job's top choice. In this case, the job-proposes version of propose and reject gives a completely different matching than the candidate-proposes version, but both are stable matchings.

3. In a job optimal stable matching, some job always gets matched to its top candidate.
   Answer: False.
   You can't create a counter-example with 2 jobs/candidates, but you can with 3:

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

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

   The propose and reject algorithm, which gives the job-optimal matching, does:
   Day 1, 1 rejects C, giving A:2, B:1, C:-
   Day 2, 2 rejects A, giving A:-, B:1, C:2
   Day 3, 1 rejects B, giving A:1, B:-, C:2
   (*note that now every job has been rejected by its top candidate...*)
   Day 4, 2 rejects C, giving A:1, B:2, C:-
   Day 5, C offers to 3 giving A:1, B:2, C:3
   In this instance, no job is matched to its top candidate.

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

   Answer: True. Consider an instance where all but one job list different candidates as their top choice, and each of those candidates lists the corresponding job first. The final job lists the remaining candidate last, and will get rejected by every other candidate since they have their top choice on a string from day 1. In the end, that job is matched with their least favorite candidate.

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

   Answer: False. Consider an instance in which both Job A and Job B list Candidate 1 as their top choice, and Candidate 1 prefers Job B. If Job A were matched to Candidate 1 (its favorite), then Job B and Candidate 1 would be a rogue pair.

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

   Answer: False. If all jobs list different candidates as their top choice, then all candidates receive a single offer on day 1, accept, and the algorithm halts. The candidate rankings are irrelevant to the propose and reject algorithm in this case.

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.

   Answer: Create an instance in which each job lists a different candidate as their top choice, and then set up the candidate lists so that each candidate's preference list makes the job that prefers them their least favorite. The candidate rankings are irrelevant (as in the preceding true/false question), so each candidate ends up paired with 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.
   Answer: False. The smallest connected graph is a tree, and a tree with 6 vertices has $|V| - 1 = 5$ edges.

   (b) A 6-vertex graph with 6 edges is connected.
   Answer: Could be either. A 6-vertex tree with an extra edge added is connected, but two triangles (two copies of K_3) have 6 edges and is not connected.

   (c) A 6-vertex graph with 6 edges is acyclic.
   Answer: False. A tree is the largest acyclic graph, and a 6-vertex tree has 5 edges.

   (d) A 6-vertex graph with 13 edges is connected.
   Answer: True. A graph that is not connected must have a cut that separates connected components. Starting from K_6, which has 15 edges, the smallest cut has 5 edges (separating out one node). Therefore, the largest 6-vertex graph that is not connected has 10 edges.

   (e) A 6-vertex graph with 13 edges is planar.
   Answer: False. Any planar graph satisfies $|E| \leq 3|V| - 6$, and in this case $3|V| - 6 = 12$. There are too many edges for this to be planar.

   (f) What is the maximum number of edges in a 6-vertex graph?
   Answer: 15. This is K_6, which has $\frac{|V|(|V|-1)}{2} = 15$ edges.

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 $|C|$?

   Answer: $|V| - |C|$

   To minimize the number of edges in a connected component, the component must be a tree. If there are $|C|$ trees with $V_1, \ldots, V_{|C|}$ vertices in each one, the number of edges is

$$\sum_{i=1}^{|C|} (|V_i| - 1) = \left(\sum_{i=1}^{|C|} |V_i| \right) - |C| = |V| - |C|.$$

3. The questions below deal with the graph K_7.

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

   Answer: True.

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

   Answer: K_7 is connected, and every vertex in K_7 has degree 6, which is even. All vertices having even degree is a sufficient condition for a connected graph to have an Eulerian tour.

4. The questions below deal with the graph K_8.

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

   Answer: False.

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

   Answer: K_8 is connected and every vertex has degree 7, which is odd. If a graph has any vertex of odd degree then it does not have an Eulerian tour.

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

   Answer: 17

   Euler's formula says that a connected planar graph with v vertices, e edges, and f faces, must satisfy $v + f = e + 2$, or $e = v + f - 2$. In this case $v = 15$ and $f = 4$, so plugging in we get $e = 17$.

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.

   Answer: Let $G = (V, E)$ be a graph with n vertices, and let $V = \{v_1, \ldots, v_n\}$ be the vertices. Let $\deg(v_i)$ denote the degree of vertex v_i. If all vertices have odd degree then each $\deg(v_i) = 2k_i + 1$ for some integer k_i, and the sum of the degrees is $\sum_{i=1}^{n} \deg(v_i) = \sum_{i=1}^{n} (2k_i + 1) = 2\left(\sum_{i=1}^{n} k_i\right) + n$. By the degree sum formula, we know this is twice the number of edges, so if m is the number of edges we have

$$2m = 2\left(\sum_{i=1}^{n} k_i \right) + n \implies n = 2(m - \sum_{i=1}^{n} k_i).$$

   Therefore, n is even.

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.

   Answer: We must get stuck at some vertex, since there are only a finite number of edges to traverse. Let $t \in V$ be the vertex at which we get stuck, and assume for the sake of contradiction that the degree of t is not 1. Since the graph is connected, no vertex can have degree 0, which means the degree of t is ≥ 2. Our walk can never visit the same node twice, because that would form a cycle and trees are acyclic. Therefore we have never visited t before we get stuck there, and we have only traversed one of the edges incident to t (in order go get there). But if the degree of t is ≥ 2 there must be some untraversed edge incident to t, and we are not stuck. This is a contradiction, so t must have 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 $5^{42} \bmod 41$?

   Answer: 25. Since 41 is prime, Fermat's Little Theorem says that $5^{40} \equiv 1 \pmod{41}$. Therefore, $5^{42} \equiv 5^{40} \cdot 5^2 \equiv 1 \cdot 25 \equiv 25 \pmod{41}$.

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

   Answer: 9. The last (decimal) digit is the result mod 10, so the last digit is $519^{487} \bmod 10$. Working mod 10, we can use any item from the same residue class, so we can replace 519 with 9 or -1: $519^{487} \equiv 9^{487} \equiv (-1)^{487} \pmod{10}$. Looking at successive powers of -1, it simply bounces between -1 (for odd powers) and 1 (for even powers), and since this power is odd the result is equivalent to $-1 \pmod{10}$. Therefore the last digit is 9.

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

   Answer: 43. The modulus 55 is not prime, so we can't apply Fermat's Little Theorem directly. We do the operation mod 5 and mod 11 and combine using the Chinese remainder theorem. Doing the computation mod $p = 5$, we can remove multiples of $p - 1 = 4$ in the exponent as $43^{21} \equiv 43^{4 \cdot 5 + 1} \equiv \left(43^4\right)^5 \cdot 43^1 \equiv 43^1 \pmod{5}$. Similarly, when the is 11 we can remove multiples of 10 from the exponent: $43^{21} \equiv 43^{10 \cdot 2 + 1} \equiv 43^1 \pmod{11}$. The CRT remainder theorem says the solution for $x \pmod{55}$ is unique given values mod 5 and mod 11, so 43 is the unique solution.

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 $x \not\equiv 0 \pmod{m}$.

   Answer: Any values of a and m with $\gcd(a, m) > 1$ will work. For example, we can use $a = 2$ and $m = 4$, and then $x = 2$ is a non-zero x that works ($ax \equiv 2 \cdot 2 \equiv 4 \equiv 0 \pmod{4}$). In general, for any values with $\gcd(a, m) > 1$, $x = \frac{m}{\gcd(a,m)}$ is a solution: $a \cdot \frac{m}{\gcd(a,m)} = m \cdot \frac{a}{\gcd(a,m)}$. Since a is divisible by $\gcd(a, m)$, this is an integer times m, and so is $\equiv 0 \pmod{m}$.

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

   Answer: True. Note that $(x + k) \bmod x = k$, and from the notes (Euclid) $\gcd(x, y) = \gcd(x, y \bmod x)$.

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

   Answer: False. Since $\gcd(a, m) = 1$, a has a unique multiplicative inverse mod m, and so the unique solution for x is $a^{-1}b \bmod m$.

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

   Answer: True. This means that both a and m are even, and if b is even then there are two solutions (x and $x + m/2$) and if b is odd then there are no solutions.

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?
   Answer: 7. For RSA, e must be relatively prime to $(p-1)(q-1) = 10 \cdot 6 = 60$. All values $2, 3, 4, 5, 6$ divide evenly into 60, so 7 is the smallest value relatively prime to 60.
   (b) If we use $e = 29$, what is the corresponding d?
   Answer: 29.
   Explanation: We use the hand-computation method for finding a and b with $29a + 60b = 1$ (the values were chosen to make this a short computation!)
   We start with two formulas:
   $29 \cdot 0 + 60 \cdot 1 = 60$
   $29 \cdot 1 + 60 \cdot 0 = 29$
   Multiplying the second by 2 we get
   $29 \cdot 2 + 60 \cdot 0 = 58$
   which we subtract from the first to get
   $29 \cdot (-2) + 60 \cdot 1 = 2$
   Multiplying this by 14:
   $29 \cdot (-28) + 60 \cdot 14 = 28$
   Subtracting from the second equation:
   $29 \cdot 29 + 60 \cdot (-14) = 1$
   This gives $a = 29$ and $b = -14$ as the final answer, so the multiplicative inverse of 29 $\pmod{60}$ is 29.

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 $n \in \mathbb{N}$.
   Answer: Working mod 7, we can replace 11 in the formula with 4, since $4 \equiv 11 \pmod{7}$, giving $11^n - 4^n \equiv 4^n - 4^n \equiv 0 \pmod{7}$. Therefore, $11^n - 4^n$ is a multiple of 7.
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 $b \equiv a^m \pmod{p}$.
   Answer: (*Note for Summer 2025 students: This is basically the same as "Baby Fermat" on Disc1D*)
   Let a and p be as in the problem statement, and assume for the sake of contradiction that there is a non-zero b such that there is no non-negative $m < p-1$ such that $b \equiv a^m \pmod{p}$. Consider the values $a^0, a^1, \ldots, a^{p-2} \pmod{p}$, which is a list of $p-1$ non-zero values. Since there are exactly $p-1$ non-zero values $\pmod{p}$ and one of them (b) is not in that sequence, by the pigeon hole principle some value must appear more than once. Define $0 < i < j < p-1$ such that $a^j \equiv a^i \pmod{p}$.
   Now consider $a^{j-i} \pmod{p}$. We can multiply out $a^{j-i} \cdot a^i \equiv a^j \pmod{p}$, and since $a^j \equiv a^i \pmod{p}$ we have $a^{j-i}a^i \equiv a^i \pmod{p}$. Since a^i is non-zero and the modulus is prime, a^i has a multiplicative inverse and we can cancel a^i from both sides to get $a^{j-i} \equiv 1 \pmod{p}$. Since $0 < i < j < p-1$, we know that $1 \leq j - i < p-1$, which contradicts the requirement in the problem statement that $a^k \not\equiv 1 \pmod{p}$ for all $1 \leq k < p-1$. Our initial assumption led to a contradiction, so there is no such b.
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.
   Answer: We multiply out $(m-1)^2 = m^2 - 2m + 1 = (m-2)m + 1$. Therefore, $(m-1)^2 = km + 1$ for integer $k = m-2$, and so $(m-1)^2 \equiv 1 \pmod{m}$.

(b) $(m-1)$ is a non-trivial square root of 1 $\pmod{m}$.
Answer: False. $m-1 \equiv -1 \pmod{m}$, so $m-1$ is a trivial square root of 1 mod m.

(c) (8 points) Prove that for prime modulus p, there are no non-trivial square roots of 1.
Answer: Any square root of 1 mod p satisfies the equation $x^2 \equiv 1 \pmod{p}$, so $x^2 - 1 = kp$ for some $k \in \mathbb{Z}$. Factoring the left side, we get $(x-1)(x+1) = kp$. Since p is prime, it has no factors in the range $2, \ldots, p-1$, so the only way $(x-1)(x+1)$ could be a multiple of p, with $x \in \{0, \ldots, p-1\}$, is if $x-1=0$ or $x+1=p$. In the first case, $x \equiv 1 \pmod{p}$ and in the second case $x \equiv -1 \pmod{p}$, so in either case x is a trivial square root of 1 mod p.

(d) Give a non-trivial square root of 1 $\pmod{15}$.
Answer: 4 or 11. 4 is the obvious one, since $4^2 = 16$ which is $15+1$.

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 $P(x) - Q(x)$?
   Answer: $\max(d_1, d_2)$. As long as the highest degree term doesn't cancel out in $P(x) - Q(x)$ it remains the degree of the difference.

   (b) What is the minimum possible degree of $P(x) - Q(x)$?
   Answer: 0. All except the constant degree term could cancel, leaving with $P(x) - Q(x)$ being a constant, which is a degree 0 polynomial.

   (c) What is the maximum number of different x values for which $P(x) = Q(x)$?
   Answer: $\max(d_1, d_2)$. This is the same as the maximum degree of $P(x) - Q(x)$.

   (d) What is the minimum number of different x values for which $P(x) = Q(x)$?
   Answer: 0. This is the same as the minimum degree of $P(x) - Q(x)$.

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?
   Answer: 1. Recovery with 2 people, and two points define a line.

   (b) Alice and Bob are given shares $(1,6)$ and $(2,2)$. What is the secret?
   Answer: 3. The slope of this line is $2-6 \equiv -4 \equiv 3 \pmod{7}$, and so $P(0) \equiv 6-3 \equiv 3 \pmod{7}$.

   (c) If Carol has share $(3, y)$, what is y?
   Answer: 5. Using the slope of 3, $P(3) \equiv P(2)+3 \equiv 2+3 \equiv 5 \pmod{7}$.

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.

   Answer: Person 1 receives $k-1$ shares from other people, and constructs the interpolating polynomial through those $k-1$ points and the point $(0, v)$. This gives a degree $k-1$ polynomial, and their fake share is then $(1, P(1))$ which they transmit to everyone else. Since there is only one polynomial of

degree $k-1$ through k given points, all of the participants compute the same polynomial $P(x)$ from the given points, and since $P(0) = v$ they all compute v as the secret.

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?
   Answer: $n+2k$
   (b) The message is encoded using polynomial $P(x)$ – what is the degree of $P(x)$?
   Answer: $n-1$
   (c) What is the degree of the error locator polynomial $E(x)$ in the reconstruction algorithm?
   Answer: At most k (the "at most" part can be optional).
   (d) If we only had $m < k$ errors, then how many roots does $E(x)$ have?
   Answer: m
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?
   Answer: $\frac{5}{3}n$.
   Explanation: We transmit $n+2k$ packets, and since 20% can be corrupted there may be $\frac{1}{5}(n+2k)$ corrupted packets. We can correct for up to k corrupted packets, so we need $k \geq \frac{1}{5}(n+2k)$. Simplifying this to a bound on k we get $k \geq \frac{1}{3}n$, so we send $n+2k \geq \frac{5}{3}n$ packets. (Note for the Summer 2025 class: This is a specific case for the general analysis you did in question 7b of Homework 2.)

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?
   Answer: $\binom{14}{7}$. To reach the top right corner from the bottom left, we need to have made a total of 7 "up" moves and 7 "right" moves, in some order. Counting paths is the same as counting the number of ways you can place 7 "up"s in a length 14 sequence of moves, which is $\binom{14}{7}$.
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?
   Answer: $\binom{52}{7}$. This is just choosing 7 items from 52, where order doesn't matter, which is exactly what the "n choose k" notation is for.
3. How many different anagrams of the word ADDED are there? (An anagram is a rearrangement of the letters.)
   Answer: $\frac{5!}{3!}$. This is 20, but you didn't need to simplify to that. There are 5! rearrangements of the letters (first rule of counting) and each arrangement has 3! equivalent rearrangements of the "D"s so divide that out (second rule of counting).
4. How many anagrams of the word AARDVARK are there?
   Answer: $\frac{8!}{3!2!}$. 8 letters, and any of the 3! rearrangements of the A's and any of the 2! rearrangement of the R's is equivalent.

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

   Answer: 6^{10}. At every roll, there are 6 possible outcomes. There are 10 rolls, so by the first rule of counting the number of different sequences is $6 \times 6 \times \cdots \times 6 = 6^{10}$.

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?

   Answer: $\binom{15}{5}$. This is what we called a "stars and bars" problem in lecture, where you have 10 stars (for the 10 rolls) and 5 bars (separating out the 6 counts). So the stars-and-bars pattern is 15 characters long, and you need to choose the locations for the 5 bars. Note that $\binom{15}{10}$ is also correct.