CS 70 Discrete Mathematics and Probability Theory
Spring 2025 Rao

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. **Warmup**

(1 point) How many TAs does CS70 have this semester?

Answer: 12. If you did not know this number, question 9.3 would have given you the answer as well!

3. **Propositions**

1. Let P, Q, and R be propositions. Determine whether the following statements are true or false.

(a) $(\neg P \wedge R) \vee (\neg P \wedge Q) \equiv \neg P \wedge (R \vee Q)$.
Answer: True. This is the distributive property of $\wedge$ across $\vee$.

(b) $(P \wedge Q) \wedge (\neg P \vee \neg Q) \equiv P \wedge \neg P$.
Answer: True. The statement is equivalent to $(S \wedge \neg S)$ where $S = (P \wedge Q)$, and the $\neg S = \neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$.

(c) $((P \implies Q) \wedge (P \implies \neg Q)) \equiv \neg P$.
Answer: True. The statement is the form of proof by contradiction. If P implies $Q \wedge \neg Q$, it is means $P \implies False$, or its contraposition, $True \implies \neg P$.

(d) $((P \implies R) \wedge (P \implies \neg R)) \equiv \neg R$.
Answer: False. It is equivalent to $\neg P$. R could be true or false regardless of the value of P.

2. Let $P(n)$ and $Q(n)$ be predicates on $n \in \mathbb{N}$.

(a) What is the negation of $(\forall n \in N)(P(n))$? (Your answer must not use $\forall$.)
Answer: $\exists n \in N, \neg P(n)$

(b) Is the following statement true for all propositions $P(n)$?

$$[\neg(\forall n \in \mathbb{N})(P(n)) \wedge P(0)] \implies (\exists n \in \mathbb{N})(P(n) \wedge \neg P(n+1)).$$

Answer: True. This states that if $P(0)$ is true, but $P(n)$ is not always true, there must be some natural number where $P(n)$ is true and the next one is not true. This is useful with the well ordering principle as a proof technique. That is if there is no smallest counterexample, the statement $P(n)$ is true for all n.

(c) $(\forall n \in \mathbb{N})(Q(n) \wedge P(n)) \equiv (\forall n \in \mathbb{N})(Q(n)) \wedge (\forall n \in \mathbb{N})(P(n))$
Answer: True. Both $P(n)$ and $Q(n)$ must always be true for both sides.

(d) $(\forall n \in \mathbb{N})(Q(n) \implies P(n)) \equiv (\forall n \in \mathbb{N})(\neg Q(n)) \vee (\forall n \in \mathbb{N})(P(n))$
Answer: False. $Q(n)$ and $P(n)$ could be both be true on even n and false on odd, which makes the left hand side true, and the right hand side false.

4. Short proofs or counterexample.

1. (5 points) Prove the following statement or give a counterexample. Given 3 people, where each person likes exactly one other person, there is always someone that no one likes.

   Answer: False. Counterexample: Person A likes person B, person B likes person C, and person C likes person A.

2. (10 points) Let (a,b,c) be a *primitive right triangle*, meaning that $a,b,c > 0$ are integers that satisfy the Pythagorean theorem

   $$a^2 + b^2 = c^2,$$

   and all three values are coprime.

   Prove that the length of the hypotenuse c of any *primitive right triangle* must be odd.

   Answer: Note that this problem was originally intended to say that a, b, and c *together* do not have any common divisors, i.e. $\gcd(a,b,c) = 1$. In grading this question, we have allowed either interpretation.

   We can consider all the cases of the parity of a and b.

   Case 1: Both a and b are even. Then, $4 \mid a^2$ and $4 \mid b^2$, which means that $4 \mid a^2 + b^2$. This implies that $4 \mid c^2 \implies c$ is even. This contradicts the fact that a, b, and c share no common divisors, since they all share a common factor of 2—as such, it is not possible for both a and b to be even.

   Case 2: Both a and b are odd. In this case, c cannot be odd, so it's only possible for c to potentially be even: this means that we have $a = 2i+1, b = 2j+1, c = 2k$ for some $i,j,k \in \mathbb{N}$.

   Here, we have $a^2 + b^2 = 4i^2 + 4i + 1 + 4j^2 + 4j + 1 = 4k^2 = c^2$. Taking mod 4, we have $2 \equiv 0 \pmod 4$ which is a contradiction. As such, it is not possible for both a and b to be odd.

   Case 3: Exactly one of a or b is odd. WLOG, suppose a is odd and b is even. This means that a^2 is odd and b^2 is even as well, making c^2 odd as well. This in turn means that c must be odd as well.

   Across all of these cases, we've shown that c must always be odd—in fact, it must be the case that exactly one of a or b is odd.

5. Induction.

(15 points) Prove that $\forall n \in \mathbb{N}$, we have $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$.

Hint: You may use the fact that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. *You should not need to expand* $(n+1)^3$.

Answer: Base Case: For $n = 1$, $1^3 = 1 = (1)^2$
Induction Hypothesis: $\sum_{i=1}^{n} i^3 = (\frac{n(n+1)}{2})^2$ (using hint.)

Induction Step: Prove $\sum_{i=1}^{n+1} i^3 = (\frac{n(n+1)}{2})^2$ (again, using hint.)

$$\begin{aligned}
\sum_{i=1}^{n+1} i^3 &= \sum_{i=1}^{n} i^3 + (n+1)^3 \\
&= \left(\sum_{i=1}^{n} i\right)^2 + (n+1)^3 \\
&= \left(\frac{n(n+1)}{2}\right)^2 + \frac{4(n+1)^3}{4} \\
&= \frac{n^2(n+1)^2 + 4(n+1)^3}{4} \\
&= \frac{(n+1)^2(n^2 + (4(n+1)))}{4} \\
&= \frac{(n+1)^2(n+2)^2}{4} \\
&= \left(\frac{(n+1)(n+2)}{2}\right)^2 \\
&= \left(\sum_{i=1}^{n+1} i\right)^2
\end{aligned}$$

Alternative Inductive Step: Recall the identity $(a+b)^2 = a^2 + b^2 + 2ab$. Then, set $a = (1+2+\cdots+n), b = n+1$. Then, it suffices to show that $(n+1)^3 = 2(n+1)(1+\cdots+n) + (n+1)^2$. This is true because:

$$\begin{aligned}
&2(n+1)(1+\cdots+n) + (n+1)^2 \\
&= 2(n+1)\frac{n(n+1)}{2} + (n+1)(n+1) \\
&= n(n+1)^2 + (n+1)^2 \\
&= (n+1)^2(n+1) \\
&= (n+1)^3
\end{aligned}$$

6. Stable Matching.

In the following parts, we consider stable matching instances with n jobs and n candidates.

1. Out of all possible stable matching instances, what is the maximum number of rogue couples in any pairing? (Your answer should be in terms of n.)

   Answer: There could be $n(n-1)$ rogue pairs as every job and candidate pair not in a pairing could be rogue if every person is matched to their least favorite person. This is the unstable pairing from discussion!

2. If a stable matching is optimal for a job, it is pessimal for the candidate it is paired with.

   Answer: True. Suppose there is another stable pairing (J', C) where C prefers J over J'. Then, (J, C) would be a rogue couple because J also prefers C over any possible partner.

3. In the propose and reject algorithm with jobs proposing, if a candidate C rejects $n-1$ jobs, then C is paired with their favorite job.

   Answer: True. She prefers this job to every other job as she had the option to choose every other job.

4. In the propose and reject algorithm with jobs proposing, if a job J is rejected by candidate C and a different job J' is paired with C, then J ends up with a worse ranked candidate in their ordering than J'. (The rank of a candidate is the position in the job's list. It's worse if it is lower on their preference list.)

   Answer: False. On the first day, J could propose to C, J' could be rejected by $n-2$ other candidates and then ask C who rejects J, who then asks their next candidate who may accept this job.

5. (a) In a stable matching instance, if job J and candidate C each put each other at the top of their respective preference lists, then J must be paired with C in every stable matching.

   Answer: True. In any other pairing, they would be a rogue couple as they clearly prefer each other to their partners.

   (b) (4 points) Prove that for every $n \geq 2$, there exists a stable matching instance with **only one** stable matching.

   Answer: If we have (J_1, C_1) place each other at the top of each others preference lists, (J_2, C_2) do the same, etc., then the only stable matching must be $\{(J_1, C_1), (J_2, C_2), \ldots, (J_n, C_n)\}$.

   Alternate Solution: If all jobs share the same preference list $C_1 > C_2 > \cdots > C_n$ and all candidates share the same preference list $J_1 > J_2 > \cdots > J_n$, then the the same result applies, as seen in the homework.

   (c) (5 points) Prove that for every $n \geq 2$, there exists a stable matching instance with **exactly two** stable matchings.

   Answer: For the following $n = 2$ stable matching instance:

Jobs	Preferences
J_1	$C_2 > C_1$
J_2	$C_1 > C_2$

Candidates	Preferences
C_1	$J_1 > J_2$
C_2	$J_2 > J_1$

   We can see that there are exactly 2 stable matchings, $\{(J_1, C_1), (J_2, C_2)\}$ and $\{(J_1, C_2), (J_2, C_1)\}$.
   Now, for an arbitrary n, construct the preference lists for (J_1, J_2, C_1, C_2)'s to look exactly like the $n = 2$ case, and the rest of the jobs and candidates will be placed lower on these preference lists.
   For the rest of the (J_k, C_k) pairs with index $k > 2$, have them place each other at the top of their preference lists, such that they must be paired together in any stable matching.
   Thus, the only possible stable matchings can be $\{(J_1, C_1), (J_2, C_2), (J_3, C_3), \ldots, (J_n, C_n)\}$ and $\{(J_1, C_2), (J_2, C_1), (J_3, C_3), \ldots, (J_n, C_n)\}$. In other words, the two distinct stable matchings come from the base case, and all other J, C pairs with indices > 2 will be paired together.

7. Graphs

All graphs are simple and undirected unless otherwise specified.

1. Consider a connected planar graph G with a planar drawing with f faces, v vertices, and e edges.

   (a) Suppose $v \geq 3$. What is the maximum number of faces in G, in terms of v?

   Answer: The maximum number of edges is $3v - 6$ and $f = e - v + 2$ so $f = 2v - 4$.

   Now, suppose every cycle in G has at least g edges.

   (b) The number of edges in G is at most

$$\frac{g}{g-2}v - \underline{\hspace{2cm}}.$$

   (Give a tight bound.)

   Answer: $2\frac{g}{g-2}$. Recall that the equation $v + f = e + 2$ holds for connected planar graphs. Then, we note that since every cycle has at least g edges, then every face has at least g sides, and thus $f \cdot g \leq 2e$ which implies $f \leq 2\frac{e}{g}$.

Plugging this back into Euler's equation, we get:

$$e+2 \leq v+2\frac{e}{g}$$
$$e\left(1-\frac{2}{g}\right) \leq v-2$$
$$e\left(\frac{g-2}{g}\right) \leq v-2$$
$$e \leq \frac{g}{g-2}(v-2)$$

Note that for a disconnected planar graph with k connected components, it is instead true that $v+f=e+k+1>e+2$, and thus it is still true that $e+2<v+f$, and the rest of the proof follows analogously. Thus, this result can still be applied to a disconnected planar graph G.

(c) (5 points) Prove that if g is at least 6, then the graph is 3 colorable.

Answer: From the previous part, plugging in $g=6$, we can conclude that the number of edges is at most $\frac{6}{4}(v-2)$, which is less than $\frac{6}{4}v$. Note that the function from part (b) is a valid upper bound using $g=6$, because the function only decreases as g increases.

By the handshaking lemma, we know that $\sum_i \deg(v_i) = 2e < 2\times\frac{6}{4}v$. Then, the average degree is $\frac{1}{v}\sum_i \deg(v_i) < 2\times\frac{6}{4}$.

Thus, one can always find a degree ≤ 2 vertex (if there were no vertices of degree ≤ 2, then all vertices are at least degree 3, and thus the average degree would be at least 3).

We proceed with a proof by induction on v, the number of vertices.

Base Case ($n=2$): Any 2 vertex graph is 2 colorable, and thus also 3 colorable.

Strong Induction Hypothesis: Assume that every $v\leq n$ vertex connected planar graph where every cycle has at least g edges is 3 colorable.

Induction Step: Consider an arbitrary $n+1$ vertex connected planar graph where every cycle has at least g edges. Using the result established earlier, there must be a degree ≤ 2 vertex, that we now remove. Note that removing a vertex cannot decrease the number of edges in a cycle (it may potentially disconnect a cycle, but that is fine). If removing this vertex does not disconnect the graph, we can directly apply the inductive hypothesis. Elsewise, if removing the vertex does disconnect the graph, we can apply the strong inductive hypothesis to both components to 3 color each of them. Now, when adding back the vertex, it has at most two neighbors of potentially different colors, so there is still a color reserved for this vertex.

Alternate Solution: If you prove that the previous part still holds even for a disconnected graph G, then there is no need to do strong induction; weak induction will suffice.

2. Recall that the complement of a graph $G=(V,E)$ is a graph $\overline{G}=(V,\overline{E})$ on the same vertex set V with an edge $(u,v)\in\overline{E}$ if and only if $(u,v)\notin E$.

(a) Let G be a tree on n vertices. How many edges are in the complement of G?

Answer: $\binom{n}{2}-n+1$. We can subtract the number of edges in a tree from the number of edges in a complete graph. Since there are $\binom{n}{2}$ edges in a complete graph and $n-1$ edges in a tree, we have $\binom{n}{2}-n+1$ edges in the complement of a tree.

(b) Let G be a d-dimensional hypercube. How many edges are in the complement of G?

Answer: $\binom{2^d}{2}-d2^{d-1}$. This is the total number of edges in a complete graph on 2^d vertices minus the number of edges in a hypercube of dimension d.

3. The *double* of a graph $G=(V,E)$ is the graph G', constructed by making a copy of the original graph (including all edges), and connecting corresponding vertices across the two copies with an edge.

Formally, $G' = (V \cup V', E')$ where $v' \in V'$ corresponds one-to-one to each $v \in V$, and $E' = \{(v, v') \mid v \in V\} \cup \{(u,v), (u', v') \mid (u,v) \in E\}$.

(a) In a graph G with n vertices and m edges, how many edges are in its double, G'? (Your answer should be in terms of n and m.)
Answer: $2m + n = 2|E| + |V|$. Making a copy of the graph doubles the number of edges. Then, we add an edge for every pair of vertices across these two copies, which adds another n edges.

(b) If G is bipartite, then G' is bipartite.
Answer: True. Any cycle in the the new graph corresponds to a tour in the original graph, along with edges between the copies. Since the cycle must return to the original node the number of edges between copies is even. Thus, the cycle has an even number of edges that correspond to edges in the original graph and an even number between the copies, which is even.

(c) The d-dimensional hypercube is the graph formed by doubling a k-dimensional hypercube ______ times. (You may assume that $k < d$.)
Answer: $d - k$. The doubling operation is essentially the recursive operation that one uses to build the d-dimensional hypercube from the $(d-1)$-dimensional hypercube.

(d) If one doubles a n-vertex tree, what is the minimum number edges that must be removed from the doubled graph to ensure that it is acyclic?
Answer: $n - 1$. There are n edges between the two copies. 1 is sufficient to connect the graph. Removing $n - 1$ removes all cycles. It is the minimum becuase the maximum number of edges in a $2n$ vertex graph taht one can have to be acyclic is $2n - 1$ which is what we achieve.

(e) If a graph is $c \geq 2$ vertex colorable, then its doubled graph is _______ vertex colorable. (Fill in the blank with the smallest value, possibly in terms of c and/or the number of vertices n and edges m in the original graph.)
Answer: c. One can rotate the colors in the copies. Now the edges in the copy are properly colored and the edges in between are properly colored.

(f) If a graph contains a Hamiltonian cycle and has at least two vertices, then its doubled graph also contains a Hamiltonian cycle.
Answer: True. One can take the Hamiltonian tours in the base graph, and take the endpoints of an edge (u, v) and traverse one tour from v to u without the edge and then cross to u' and traverse to v' and cross to u to obtain a Hamiltonian cycle.

(g) If a graph contains an Eulerian tour and has at least two vertices, then its doubled graph also contains an Eulerian tour.
Answer: False. Recall that the condition for an Eulerian Tour is that the planar graph must have all even degree vertices. In the doubled graph, each vertex gets one new edge, so all vertices will have odd degree - thus the graph cannot have an Eulerian Tour.

8. Graph: proof.

(8 points) Let $G = (V, E)$ be a disconnected graph. Prove that its complement $\overline{G} = (V, \overline{E})$ is connected. (Recall that the complement of a graph is defined such that for $u, v \in V$, $(u, v) \in E$, if and only if $(u, v) \notin \overline{E}$.)

Answer: Given vertices $u, v \in \overline{G}$, we argue there is a path between u and v as follows.

- Case 1: If u, v is not an edge in G, then u, v is connected by an edge in $\overline{G}$.
- Case 2: If u, v is connected by an edge in G, then u, v lies in the same connected component. Pick another vertex w in another component which must exist as G is disconnected. Since the edges uw, wv are not in G, uw, wv are edges in $\overline{G}$, so there exists a path $u \to w \to v$.

Note: A common mistake is to assume that because G is disconnected, there is a vertex with 0 edges. This is not true—G being disconnected just means that there exists some vertices u, v that don't have a path between them. An example could be two copies of K_5.

Alternate Inductive Proof:

For the sake of brevity, we will just include the inductive step. Consider an arbitrary $n+1$ vertex disconnected graph G.

Cases: If G has no edges, then $\overline{G}$ is a complete graph, and thus must be connected.

Elsewise, there must be a vertex v with at least one edge. Remove v and its corresponding edges, call this new graph G'. The only way G' could possibly be connected is if the number of connected components was reduced from 2 to 1, which only occurs if v was an isolated vertex. Since v has at least one edge, this is not the case.

G' is a disconnected graph on n vertices, and thus we can apply the inductive hypothesis, implying that $\overline{G'}$ is connected. Then, we add back the vertex v to $\overline{G'}$ and all of its corresponding edges that don't exist in G, which gives us exactly $\overline{G}$. v has at least one edge in $\overline{G}$ (elsewise, v is connected to every vertex in G, which contradicts G being disconnected), and thus $\overline{G}$ is connected as well.

9. Modular Arithmetic

1. What is the inverse of $5 \pmod{24}$? Your answer should be a number in the set $\{0, 1, \ldots, 23\}$.
   Answer: 5. $5 \times 5 = 25 = 1 \pmod{24}$
2. What is $2^{75} \pmod{35}$? Your answer should be a number in the set $\{0, 1, \ldots, 34\}$. (Hint: think about RSA with $p = 7$, $q = 5$ and $e = 5$.)
   Answer: $2^{75} = (2^{25})^3 = (2)^3 = 8 \pmod{35}$. This is due to $25 = ed$, and $a^{ed} = a \pmod{pq}$ in RSA.
3. (8 points) Recall that RSA can also be used as a *signature scheme*. That is, we can use an RSA scheme to verify that a message actually came from the sender we expect.

   Professor Rao has created an RSA scheme with public key $(N, e) = (55, 3)$, and an unknown private key d.

   Professor Rao has sent you a message containing the answer to Question 2 on this exam (the number of TAs), but a hacker has also sent you another message trying to trick you into giving the incorrect answer. Professor Rao's message is of the form $(m, m^d \pmod{N})$, corresponding to his RSA scheme, and you'd like to verify which message actually came from Professor Rao.

   Suppose you received the messages $(12, 23)$ and $(13, 23)$. What message m did Professor Rao actually send you? Justify your answer. (Hint: Your calculations may be easier if you utilize CRT. You do not need to solve for d.)

   Answer: 12. Note that $(m^d)^e \equiv m^{de} \equiv m \pmod{N}$, just as in RSA, so it suffices to check whether $23^3 \pmod{55}$ is 12 or 13. As the hint suggests, we may want to consider this quantity modulo 5 and modulo 11.

   Note that if $m^{de} \equiv m \pmod{55}$, then $m^{de} \equiv m \pmod{11}$ as well. We see that $12 \equiv 1 \pmod{11}$, and $23^3 \equiv (-1)^3 \equiv 1 \pmod{11}$. However, $13 \equiv 1 \not\equiv 2 \pmod{11}$, therefore the message cannot be 13, and it has to be 12.

   A similar line of reasoning can be applied under modulo 5: we know that $12 \equiv 2 \pmod{5}$, and $23^3 \equiv 3^3 = 27 \equiv 2 \pmod{5}$ as well. On the other hand, $13 \equiv 3 \not\equiv 2 \pmod{5}$, and thus the message cannot be 13.
4. If $y < x$, then $x \,\%\, y \leq x/2$. (Recall, $x \,\%\, y$ is the remainder of x divided by y; in other words, $x \,\%\, y$ is defined as $x - \lfloor x/y \rfloor \times y$.)

Answer: True. We consider the cases.
Case 1: $y < x/2$. In this case, $x \% y < y < x/2$.
Case 2: $y \geq x/2$. In this case, $x \% y \leq x - y \leq x - x/2 \leq x/2$.

5. Recall that in the extended Euclidean algorithm, given $x, y \in \mathbb{Z}$ with $d = \gcd(x, y)$, we are able to find a, b such that
$$d = ax + by.$$
Throughout this problem, d, a, b, x, y are constants that satisfy the above equation.
   (a) Suppose i is another constant; consider the equation $zx \equiv id \pmod{y}$. What is a solution for z? (Your answer can *only* be in terms of a, b, d, and/or i.)
   Answer: ai. Since $d = ax + by$, we have $id = axi + byi = aix \pmod{y}$. Thus, $z = ai$ satisfies the equation.
   (b) How many solutions for z are there to $zx \equiv id \pmod{y}$ for a fixed i?
   Answer: d. If there is one solution, z, then $z_k = z + k(y/d)$ is also a solution for any k. The number of distinct solutions modulo y is thus d.
   (c) Suppose $\gcd(x, y) = 1$. If $z \equiv i \pmod{x}$ and $z \equiv j \pmod{y}$, give an expression for $z \pmod{xy}$ using a, b, i, x, y and/or j. (Your answer may not include any unsimplified inverses.)
   Answer: $iby + jax \pmod{xy}$. We are using the Chinese Remainder Theorem except we notice $b \equiv y^{-1} \pmod{x}$ and $a \equiv x^{-1} \pmod{y}$.

6. Suppose p is a prime. We will prove that for $a \not\equiv 1 \pmod{p}$, $a^k \equiv 1 \pmod{p} \implies \gcd(k, p-1) > 1$.
   (a) What is the smallest positive integer k where $2^k \equiv 1 \pmod{7}$?
   Answer: 3. $2^3 \equiv 8 \equiv 1 \pmod{7}$
   (b) (4 points) Prove that $a^k \equiv a^{k \bmod (p-1)} \pmod{p}$.
   Answer: Since $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's theorem, we have $a^{k \pmod{p-1}} \equiv a^{k+i(p-1)} = a^k(a^{p-1})^i \equiv a^k(1)^i \equiv a^k \pmod{p}$.
   (c) If $\gcd(k, p-1) = 1$, then $f(x) = kx \pmod{p-1}$ is a bijection from $\{1, \dots p-1\}$ to $\{1, \dots, p-1\}$.
   Answer: True. k has an inverse modulo $p-1$ and thus there is an inverse function and thus the function is 1-to-1. As the domain and co-domain are the same size this is a bijection.
   (d) (8 points) Prove that if $a^k \equiv 1 \pmod{p}$, then either $\gcd(k, p-1) > 1$ or $a \equiv 1 \pmod{p}$. (Hint: Consider $a^{ki \bmod p-1}$ for $i \in \{1, \dots p-1\}$.)
   Answer: Consider the cases. If $\gcd(k, p-1) > 1$ then the statement is true.
   Elsewise, suppose that $a^k \equiv 1 \pmod{p}$ and $\gcd(k, p-1) = 1$. We now wish to show that $a \equiv 1 \pmod{p}$.
   Since $\gcd(k, p-1) = 1$, k has an inverse x mod $p-1$ such that $kx \equiv 1 \pmod{p-1}$, or equivalently $kx = 1 + l(p-1)$ for some integer l. Note that by FLT, $a^{l(p-1)} = (a^{p-1})^l \equiv 1 \pmod{p}$, so that
$$a = a^1 \equiv a^{1+l(p-1)} = a^{kx} = (a^k)^x \equiv 1^x = 1 \pmod{p}.$$
   Alternate Solution: By (c) we know that the set $S_1 = \{a^{ki \bmod p-1} \bmod p \mid 1 \leq i \leq p-1\}$ is the same as the set $S_2 = \{a^i \bmod p \mid 1 \leq i \leq p-1\}$. Additionally, $ki \bmod p-1 = ki + l_i(p-1)$ for some integer l_i.
   Therefore,
$$a^{ki \bmod p-1} = a^{ki+l_i(p-1)} = a^{ki}(a^{p-1})^{l_i} \equiv a^{ki} \equiv (a^k)^i \equiv 1 \pmod{p}.$$
   Therefore, $S_1 = \{1\}$, and so $S_2 = \{1\}$, which in particular implies that $a^1 \equiv 1 \pmod{p}$.

(e) Suppose $a^k \equiv 1 \pmod{p}$. If $a \not\equiv 1 \pmod{p}$, then $\gcd(k, p-1) > 1$.

Answer: True. This follows directly from the previous part.

10. Polynomials.

1. (1 point each) Working under GF(5), the polynomial that passes through the points $(0,1)$, $(1,2)$, and $(2,0)$ can be written in the form ax^2+bx+c for some coefficients a, b, and c. What are the coefficients of this polynomial? (Hint: this might be easier with linear equations rather than Lagrange.)

$$a = \qquad\qquad b = \qquad\qquad c =$$

Answer: $x^2+1 \pmod{5}$. Since the polynomial passes through $(0,1)$, we know that $c = 1$. The other two equations give $a+b+1 \equiv 2 \pmod{5}$ and $4a+2b+1 \equiv 0 \pmod{5}$. Solving these equations, we have that $a = 1$ and $b = 0$.

2. Suppose we have a degree 1 polynomial $P(x)$ in GF(5). The points $(0,1)$, $(1,3)$, $(2,1)$, and $(3,2)$ are received from a communication channel that has at most 1 corruption.

(a) What is $P(x)$?
Answer: $2x+1 \pmod{5}$. We need to find a degree 1 polynomial passing through at least 3 out of the 4 points. Trying out a few subsets of points gives a solution of $2x+1 \pmod{5}$, which passes through the first, second, and fourth points.

(b) What is the error polynomial, $E(x)$?
Answer: $x-2$. The point $(2,1)$ is an error, and it corresponds to $x = 2$.

In the below parts, we are working under GF(p) for a sufficiently large prime p.

3. Suppose $P(x)$ is a polynomial of degree *exactly* $d > 0$, where $d < p$. What is the maximum number of points x_i such that $P(x_i) = 2$? (Your answer should be in terms of d. Recall that a polynomial is of degree exactly d if the leading coefficient $a_d > 0$.)
Answer: d. $P(x)-2$ has degree at most d and can have at most d roots.

4. Let $P(x)$ and $Q(x)$ be polynomials of degree *exactly* d. Moreover, $P(x)$ has r distinct roots and $Q(x)$ has r' distinct roots.

(a) What is the maximum number of distinct roots for $R(x) = P(x)Q(x)$?
Answer: $r+r'$. The roots of $P(x)$ and $Q(x)$.

(b) What is the minimum number of distinct roots for $R(x) = P(x)Q(x)$?
Answer: $\max(r, r')$. The roots of $P(x)$ and $Q(x)$. They could have the same roots.

(c) What is the degree of $P(x)Q(x)$?
Answer: $2d$. The leading term will be of the form x^{2d} and be non-zero as the non-zero leading coefficients of $P(x)$ and $Q(x)$ multiplied together is non-zero.

(d) What is the maximum degree of $P(x)+Q(x)$?
Answer: d. This is the max degree of the two polynomials.

5. (5 points) Prove that a polynomial $P(x)$ of degree exactly 1 has exactly 1 root.
Answer: $P(x) = mx+b$. One can find x where $P(x) = 0 = mx+b$, then $x = -b(m^{-1})$ is a root.

6. We will prove that there is a polynomial of degree exactly 2 with fewer than two roots.
If $P(x)$ has two roots, then $P(x) = a(x-r_1)(x-r_2) \pmod{p}$. Note that $P(x) = a(x-r_2)(x-r_1)$ is the same polynomial. Moreover, $P(x) = a(x-r)^2$ is considered to have two roots.

(a) How many polynomials of degree exactly 2 are there with two roots? Recall that we are working in GF(p). (Careful: Can a be 0?)
Answer: $(p-1)(\binom{p}{2}+p)$. Polynomials of degree two with two roots must be of the form $a(x-r_1)(x-r_2)$. There are a total of $p-1$ choices for a, since it cannot be zero. We can then pick two values in GF(p) for the two roots: there are $\binom{p}{2}$ ways of picking two (unordered) roots, and p ways of picking a double root (i.e. when $r_1 = r_2$).

(b) How many polynomials of degree exactly 2 are there?
Answer: $(p-1)p^2$. A polynomial of degree 2 can be written in the form $a_2x^2 + a_1x + a_0$. Since the polynomial must be of degree exactly 2, a_2 cannot be zero. All other coefficients can be zero, so we have a total of $(p-1)$ choices for a_2, and p choices each for a_1 and a_0.

11. Rogue Delegates.

(12 points) 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 thestable correct secret. What is the largest number of rogue delegates that can attend the conference such that the committee is guaranteed to recover the correct secret? Justify your answer.

Answer: 32 delegates.

For a degree 49 polynomial, 50 points must be received correctly, and thus 10 errors out of a total of 70 points can be tolerated. Thus, the rogue delegates must create 11 corruptions on the shared polynomial in order to corrupt the secret.

For each delegation, 6 correct points are required, and thus 8 points need to be send to counter 2 errors out of 10 points. Thus, only 3 rogue delegates are necessary to corrupt the secret.

Then, $3 \cdot 11 = 33$ rogue delegates are sufficient to corrupt the secret of the shared polynomial. Accordingly, the maximum number of rogue delegates that the committee can guard against is 32.

12. 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. How many ways can the letters in BAA be arranged?
Answer: $3 = \frac{3!}{2}$. 3! counts the possible arrangements, but we divide by 2 to account for the fact that the A's are identical.

2. How many ways can the digits in 126 be arranged?

   Answer: $6 = 3!$. 3 ways to choose the first one, 2 ways to choose the second one, and 1 way to choose the last.

3. Suppose there are n teddy bears and k children, for $n > k$. How many ways are there to assign teddy bears to the children, such that every child has a single distinct teddy bear? The bears and children are both distinguishable.

   Answer: $\frac{n!}{(n-k)!}$. There are n ways to assign to the first one, $n-1$ to the second, etc.

4. How many ways are there to assign $x_1, \ldots, x_n \in \mathbb{N}$ (which are not necessarily distinct) such that

$$x_1 + x_2 + \cdots + x_n = k,$$

   where each x_i is at least 1?

   Answer: $\binom{k-1}{k-n} = \binom{k-1}{n-1}$. Since each x_i is at least 1, this is equivalent to finding

$$(y_1 + 1) + (y_2 + 1) + \cdots + (y_n + 1) = k \implies y_1 + y_2 + \cdots + y_n = k - n,$$

   where each $y_i \geq 0$.

   Here, we have $k - n$ stars, and $n - 1$ bars, so we have $k - n + n - 1 = k - 1$ items in total, out of which we choose where the $k - n$ stars go. (Or equivalently choosing where the $n - 1$ bars go.)

5. How many n-bit strings are there with exactly k ones?

   Answer: $\binom{n}{k}$. There are n positions, and we choose k positions for the ones.

6. How many necklaces are there with n distinguishable beads? (Note that the necklace is a circle, thus ABC is the same as CAB, if one views this as a string.)

   Answer: $(n-1)! = \frac{n!}{n}$. There are $n!$ ways of ordering n objects in a line, but this does not count the cyclic symmetries—there are a total of n ways of rotating the necklace that should be equivalent, so we must divide by n.