CS 70 Discrete Mathematics and Probability Theory
Spring 2023 Rao and Ayazifar

# 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 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 product of **all** numerical student answers for this question?

**Answer:** 0. In fact, no matter what the actual product is, answering 0 will make the product of all student answers equal to 0.

**3. Propositional Logic**

True means always true regardless of the choice of predicates $P(\cdot)$ and $Q(\cdot)$ or the values of the propositions $P$ and $Q$.

1. $(\neg Q \implies (P \implies Q)) \equiv (P \implies Q)$
   **Answer:** True. $(\neg Q \implies (P \implies Q)) \equiv (Q \vee \neg P \vee Q) \equiv (\neg P \vee Q) \equiv (P \implies Q)$
2. $(\neg P \vee (P \implies Q)) \equiv (P \implies Q)$
   **Answer:** True. $(\neg P \vee (P \implies Q)) \equiv (\neg P \vee \neg P \vee Q) \equiv \neg P \vee Q \equiv P \implies Q$.
3. Write an equivalent expression for $\neg(\forall x \in S)(P(x) \implies \neg Q(x))$ that does not use the negation symbol, "$\neg$".
   **Answer:** $\neg \forall x \in S, (P(x) \implies \neg Q(x)) \equiv \exists x \in S, \neg(\neg P(x) \vee \neg Q(x)) \equiv \exists x \in S, P(x) \wedge Q(x)$.
4. Consider the following implication:

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

   (a) Is the implication true or false?
   **Answer:** True.

   (b) Give a counterexample or a proof of the implication.
   **Answer:** One can move the quantifier $(\exists x \in S)$ around $Q(x)$, as it only depends on $x$; similarly one can move the quantifier $(\forall y \in S)$ around $P(y)$, as it only depends on $y$. Doing so gives $((\exists x \in S)Q(x)) \wedge ((\forall y \in S)P(y))$ for both sides.

**4. Proofs**

1. (5 points) Prove that if a number does not leave a remainder of 0 or 1 when divided by 4, then it is not a perfect square.

   **Answer:** Proceed by contraposition. Assume a number $y$ is a perfect square. If $y$ is even then there exists some $x$ such that
   $$y = (2x)^2 = 4x^2 \equiv 0 \pmod 4.$$
   If $y$ is odd, then there exists some $x$ such that
   $$y = (2x+1)^2 = 4x^2 + 4x + 1 \equiv 1 \pmod 4.$$
   Note: We use without proof the fact from Notes and Lecture that $a^2$ is even implies $a$ is even and $a^2$ is odd implies $a$ is odd.

2. (10 points) Prove for any $N > 0$ integers, $a_1 \leq \cdots \leq a_N$, there is a subset of them that sums to a multiple of $N$.

   (Hint: Let $S_i = \sum_{k=1}^{i} a_k$, and consider the remainders of $S_1$ to $S_N$ when divided by $N$.)

   **Answer:** Following the hint, We define $S_i$ such that $S_i = \sum_{k=1}^{i} a_k$. For $S_1$ to $S_N$ when divided by $N$, the possible remainders are $\{0, 1, \ldots, N-1\}$. There's two cases from here. First, some $S_i \equiv 0 \pmod N$ in which case we're done. The other case is that none of the $S_i \equiv 0 \pmod N$. By Pigeonhole, this means that for some $i < j$ we have $S_i \equiv S_j \pmod N$. Seeing that $S_j - S_i \equiv 0 \pmod N$, we see that the subset $\{a_{i+1}, a_{i+2}, \ldots, a_j\}$ is a valid construction.

## 5. Induction I.

Recall the Fibonacci numbers: $F_1 = 1$, $F_2 = 1$, and $F_m = F_{m-1} + F_{m-2}$ for $m \geq 2$.

Consider the following theorem.

> **Theorem:** Any natural number $n$ can be written in the form
> $$n = \sum_{i=1}^{k} F_{m_i},$$
> where the $m_i$ are distinct positive integers such that **no two $m_i$, $m_j$ are consecutive**. For example, $12 = 8 + 3 + 1 = F_6 + F_4 + F_1$.

Here is a partial proof of the above theorem.

*Base cases*: For $n = 0$, the statement is vacuously true. For $n = 1$, this is true since $1 = F_1$.

*Inductive hypothesis*: For any $m \geq 2$, suppose that every number from $0 \leq n \leq m-1$ can be written in the form above.

*Inductive step*: We will prove that $m$ can be written in the form above.

Let $k$ be the largest integer such that $F_k \leq m$. Then by the inductive hypothesis, $m - F_k$ can be written as a sum of nonconsecutive Fibonacci numbers.

1. (6 points) Prove that $m - F_k < F_{k-1}$.

   **Answer:** Suppose for contradiction that $m - F_k \geq F_{k-1}$. Then $m \geq F_k + F_{k-1} = F_{k+1}$, contradicting the maximality of $F_k$.

2. (6 points) Finish the proof of the theorem using the fact above.

   **Answer:** We have $m - F_k < F_{k-1}$, so the expression of $m - F_k$ as nonconsecutive Fibonacci numbers consists of Fibonacci numbers at most $F_{k-2}$ and the expression for $m$ results from adding $F_k$.

**6. Induction II**

(12 points) Prove for all $n \geq 2$ that

$$\sqrt{2\sqrt{3\sqrt{4\cdots\sqrt{n}}}} < 3.$$

(Hint: Try proving

$$\sqrt{k\sqrt{(k+1)\cdots\sqrt{n}}} < k+1$$

for all $2 \leq k \leq n$.)

**Answer:** We prove a stronger statement. Namely, we will prove for all $2 \leq k \leq n$ that

$$\sqrt{k\sqrt{(k+1)\cdots\sqrt{n}}} < k+1.$$

The base case $k = n$ trivially follows from $\sqrt{n} < n+1$. For the induction hypothesis assume that

$$\sqrt{k\sqrt{(k+1)\cdots\sqrt{n}}} < k+1.$$

We can see that

$$\sqrt{(k-1)\sqrt{k\sqrt{(k+1)\cdots\sqrt{n}}}} < \sqrt{(k-1)(k+1)} < \sqrt{k^2} = k$$

where we use the fact that $(k-1)(k+1) = k^2 - 1 < k^2$.

Our original statement is an application of $k = 2$.

**7. Stability in Matchings.**

1. The only stable matchings are the job optimal and candidate optimal stable matchings.
   **Answer:** False. For example, one can take two 2 stable matching instances, $I_1$ and $I_2$, consisting of 2 jobs and 2 candidates with different optimal solutions for jobs and candidates and them to make a 4 job/candidate instance where the preference lists for $I_0$ have the entities in $I_1$ at the end, and vice versa for $I_1$ and $I_0$. A stable matching in the combined instance exists that corresponds to matching $I_0$ (or $I_1$) either job or candidate optimally. This yields 4 possible stable matchings for the combined instance.
2. If in a matching, candidate $c$ is paired with the first job on its preference list, it cannot be in a rogue pair.
   **Answer:** True. In a rogue pair the candidate must prefer a different job than its partner which isn't possible if its partner is first in its preference list.
3. If in a matching, candidate $c$ is paired with the last job on its preference list, it must be in a rogue pair.
   **Answer:** False. Every job could have $c$ last in it preference list and therefore every job prefers its partner at least as much as it prefers $c$.
4. If a candidate is paired with the $k$th job on its preference list in a stable matching, this candidate must not be first in the preference list for at least ___ jobs.
   **Answer:** $k-1$. If any of the $k-1$ previous jobs in its list had the candidate first, that would constitute a rogue pair.
5. Explain why the number of rejected proposals in the job-propose stable matching algorithm for an instance with $n$ jobs and $n$ candidates is at most $n(n-1)$.
   **Answer:** Every candidate can only reject $n-1$ jobs and still end up matched since no job proposes again.

## 8. Graphs

All graphs are simple and undirected unless otherwise specified.

1. The 3-dimensional hypercube has an odd number of vertices.
   **Answer:** False. A 3-dimensional hypercube has $2^3$ vertices.
2. How many faces are in a planar drawing of a $n$-vertex tree? (Possibly in terms of $n$.)
   **Answer:** 1. Trees have no cycles, so there is only one face.
3. How many faces are in a planar drawing of an $n$-vertex connected graph with exactly one cycle?
   **Answer:** 2. The cycle forms a face, and the infinite face makes 2 total faces.
4. What is the minimum degree of any vertex in an $n$-vertex tree when $n \geq 2$? (Possibly in terms of $n$.)
   **Answer:** 1. The number of edges is $n-1$ in a tree and sum of degrees is $2n-1$ and if every vertex has degree at least 2 then the sum would be at least $2n$, thus there is a degree less than 2, and since it is connected the degree of every vertex is at least 1.
5. Recall a bipartite graph is a graph, $G = (V, E)$, where $V = A \cup B$, $A \cap B = \varnothing$, and $E \subseteq A \times B$.
   (a) What is the maximum number of edges in a bipartite graph? (Possibly in terms of $|V|$, $|A|$ and $|B|$?)
   **Answer:** $|A| \times |B|$. Every edge between $A$ and $B$ can appear, and only those edges.
   (b) Every graph where every vertex has degree at most 2 is bipartite.
   **Answer:** False. The three-cycle is not bipartite.
   (c) Every bipartite planar graph with $n$ vertices has a vertex of degree at most ______. (Give a tight bound, possibly in terms of $n$.)
   **Answer:** 3. The total number of edges is at most $2n-4$, and the sum of degrees is at most $4n-8$ and thus there must be a vertex of degree at most 3 since otherwise the sum of the degrees would be at least $4n$.
   (d) A 3-dimensional hypercube $G = (V, E)$ is bipartite. Recall that the vertices correspond to bit-strings, e.g., $000, 011, 010$ are vertices in $V$. Describe a set $A$ (where $B = V - A$) such that $E \subseteq A \times B$.
   **Answer:** $\{000, 011, 110, 101\}$. In a hypercube, edges connect vertices that differ in 1 position, thus edges go between vertices with an even number of 1's to an odd number of 1's. This set consists of all vertices with an even number of 1's.
6. The *maximum* degree of any vertex in an $n$-vertex planar graph is ______.
   **Answer:** $n-1$. Any tree is planar, and the tree where one vertex has an edge to every other vertex has a vertex with degree $n-1$.
7. Consider an $n$-vertex graph where $n \geq 3$, with vertices $u$ and $v$ that have degrees $d_u$ and $d_v$ respectively. The vertices $u$ and $v$ must have a common neighbor when $d_u + d_v \geq$ ______. (Answer could be in terms of $n$. A common neighbor of $u$ and $v$ is a vertex $x$ where $(u, x)$ and $(v, x)$ are edges.)
   **Answer:** $n+1$. The total number of neighbors of $u$ and $v$ which are not $u$ or $v$ is at least $d_u + d_v - 2$. If this is larger than $n-2$ then $u$ and $v$ must share an edge. That is, $d_u + d_v - 2 \geq n-1$ and isolating $d_u + d_v$.
8. (5 points) Prove or disprove: There are at least 3 vertices of degree less than 6 in any connected planar graph with more than 100 vertices.
   **Answer:** The number of edges is at most $3v-6$ and thus the sum of degrees is at most $6v-12$ and for a connected planar graph every vertex has degree at least 1. Thus, if $v-2$ vertices have degree 6 and 2 have degree 1, the sum of degrees is $6(v-2)+2 > 6v-12$, so at least 3 vertices must have degree less than 6.

9. Consider a $n$-vertex graph $G = (V,E)$. Suppose we create a new graph $G' = G - v$ by removing a vertex $v$ of degree $d$ from $G$. If $G'$ can be vertex-colored with $k$ colors, then $G$ can be vertex-colored with at most ______ colors.

   (Give a tight bound, possibly in terms of $d$, $k$, and $n$. Max and/or min might be useful as $d$ and $k$ are possibly different.)

   **Answer:** $\max(k, 1+\min(d,k))$. The $d$ neighbors of $v$ use at most $\min(k,d)$ colors, least one is available to color $v$, which implies that a set of $1+\min(k,d)$ colors is sufficient. But, at least $k$ colors are needed to color $G'$, thus we have $\max(k, 1+\min(k,d))$

## 9. Graph: proof.

All graphs are simple and undirected unless otherwise specified.

1. Consider a graph with $n$ vertices where every vertex has degree exactly 3.
   (a) $n$ must be even.
   **Answer:** True.
   (b) Give a short proof or counterexample.
   **Answer:** The sum of degrees is $3n$ and the number of edges, $e = 3n/2$ must be an integer. Thus, $2e = 3n$ which implies $n$ must contain a factor of 2 which means it is even.
2. Consider a graph with $n$ vertices where every vertex has degree exactly 4.
   (a) $n$ must be odd.
   **Answer:** False.
   (b) Give a short proof or counterexample.
   **Answer:** Take two triangles and take each vertex in one triangle and use two edges to connect to a different pair of vertices in the other triangle. The degree is 4 and there are six vertices. FWIW, a counterexample has to have 6 vertices as for five vertices the graph must be $K_5$ and for smaller number of vertices the degree cannot be 4.
3. (5 points) Prove every $n$-vertex graph with $n \geq 2$ has at least 2 vertices with the same degree.
   **Answer:** Suppose for the sake of contradiction that no two vertices have the same degree. This means that each vertex has a different degree from the set $\{0, 1, \ldots, |V|-1\}$. However, it's impossible for one of the vertices to have degree 0 (connected to no other vertex in the graph) and one vertex having degree $|V|-1$ (connected to every vertex in the graph).

## 10. Sets and (modular) functions.

A *k-uniform* function $f : A \to B$ is a function where for each $y \in B$, either

1. there are exactly $k$ distinct values, $x_1, \ldots, x_k \in A$, where $y = f(x_i)$
2. or $(\forall x \in A)(y \neq f(x))$.

For each of the following functions, $f : A \to B$, indicate the value of $k$ for which $f$ is $k$-uniform, or "Unknown" if there is not enough information to determine $k$.

1. $A = \{0,1,2,3\}$, $B = \{0,1,2\}$, and $f : A \to B$ is defined as $f(0) = 0$, $f(1) = 0$, $f(2) = 1$, $f(3) = 1$.
   **Answer:** 2. Apply the definition, each element of $B$ is the image either 2 elements of $A$ or none.

2. For $f(x) = g(h(x))$ for a $k_1$-uniform function $g : X \to B$ and a $k_2$-uniform function $h : A \to X$. (Possibly in terms of $k_1$ and/or $k_2$.)

   **Answer:** Unknown. For $C$ it may have $k_2$ pre-images in $X$ under $g(\cdot)$, but for those they may the image of $k_1$ or 0 elements of $A$ under $h(\cdot)$. This makes it impossible to predict the number of pre-images in $A$ that eventually map to $C$ under $f(x) = g(h(x))$.

3. Below, $A = B = \{0, \dots, m-1\}$ under arithmetic modulo $m$.

   (a) $f(x) = ax \pmod{m}$ for a prime $m$ where $a \neq 0 \pmod{m}$. (Possibly in terms of $a$ and/or $m$.)
   **Answer:** 1. Since the function has an inverse, only one pre-image can correspond to each image.

   (b) $f(x) = ax \pmod{m}$ where $\gcd(a, m) = d$. (Possibly in terms of $a$, $m$ and/or $d$.)
   **Answer:** $d$. Given an $ax \pmod{m}$, we have $a(x + i(m/d)) = ax + i(a/d)m = ax \pmod{m}$, and thus $f(x) = f(x + i(m/d))$ and there are $d$ values of $i$ where $x + i(m/d)$ are different modulo $m$.

4. $f(x) = ax \pmod{m}$ where $m = pq$ for primes $p$ and $q$, $A = \{x \mid \gcd(x, m) = 1\}$, and $\gcd(a, m) = 1$. (Possibly in terms of $a$, $m$, $p$ and/or $q$.)

   **Answer:** 1. Since $f(x) = ax \pmod{m}$ is a bijection on the entire set and $a$ has no factor of $p$ or $q$ so the expression $ax$ is relatively prime to $m$ and is thus the image is always in $A$ for $x \in A$.

5. $f(x) = ax \pmod{m}$ where $m = pq$ for primes $p$ and $q$, $A = \{x \mid \gcd(x, m) = 1\}$, and $\gcd(a, m) = p$. (Possibly in terms of $a$, $m$, $p$, and/or $q$.)

   **Answer:** $p - 1$. Consider $y = ax \pmod{m}$, then $x' = x + iq$ is a solution for any $i$ since $a = kp$ and $ax + iaq = ax + ikpq = y + 0 = y \pmod{m}$. This is true for $p$ values of $i \in \{0, \dots, p-1\}$. However, one of $x + iq = 0 \pmod{p}$ for exactly one $i$ since $q$ has a multiplicative inverse modulo $p$. Thus, we get $p - 1$.

## 11. A bit more modular arithmetic.

1. If $x \equiv 3 \pmod{5}$ and $x \equiv 2 \pmod{11}$, what is $x \pmod{55}$?

   **Answer:** 13. $3(11)(11^{-1} \pmod{5}) + 2(5(5^{-1}) \pmod{11}) \pmod{55}$.

2. Consider the system of equivalences

$$\begin{cases} x \equiv a & \pmod{10} \\ x \equiv b & \pmod{15}. \end{cases}$$

   (a) If $b - a$ is a multiple of 5, what is the number of solutions for $x \pmod{150}$?
   **Answer:** For a solution, we have $x + i(30)$ is still a solution. There are 5 values of $i$ which yield different $x$'s under modular arithmetic $p$.

   (b) If $b - a$ is *not* a multiple of 5, what is the number of solutions for $x \pmod{150}$?
   **Answer:** 0. $x = a + 10k$ and $x = b + 15k'$ which means $0 = b - a + (10k - 15k') = (b - a) + 5(2k - 3k')$ thus $(b - a)$ must be a multiple of 5 since $(2k - 3k')$ is an integer.

3. Let $p$ be a prime and $a$ be an integer. Then $a^p - a$ is a multiple of $p$.

   **Answer:** True. It is divisible by $p$ as if $a$ is a multiple of $p$ the expression is, if not we have $a^{p-1} = 1 \pmod{p}$ and have $a(a^{p-1} - 1) = 0 \pmod{p}$.

4. Let $a$ be an integer and $p$ and $q$ be primes. Then $a(a^{(p-1)(q-1)} - 1)$ is a multiple of ______. (Answer should be as large as possible and cannot be 1 or involve $a$. It may involve $p$ and $q$.)

   **Answer:** $pq$. We have that $a((a^{(p-1)})^{q-1} - 1) = 0 \pmod{p}$ since either $a = 0$ or $a^{(p-1)} = 1 \pmod{p}$ and thus $a^{(p-1)} - 1$ is divisible by $p$. Same is true for $q$. Thus it is divisible by both.

5. Consider an RSA scheme with public key $(N,e)$ and private key $d$. Let $y_1 = x_1^e \pmod N$ and $y_2 = x_2^e \pmod N$.

   (a) How should the message $x_1x_2 \pmod N$ be encrypted? Express your answer in terms of $y_1$, $y_2$, $N$, $e$, and/or $d$.
   **Answer:** $y_1 \cdot y_2$. $(x_1 \cdot x_2)^e = x_1^e x_2^e = y_1y_2 \pmod N$.

   (b) Express $x_1x_2 \pmod N$ in terms of $y_1$, $y_2$, $N$, $e$, and/or $d$.
   **Answer:** $(y_1y_2)^d$. $x_1^{ed} \equiv x_1 \pmod N$ and $x_2^{ed} \equiv x_2 \pmod N$ by the RSA algorithm so $x_1x_2 \equiv x_1^{ed}vx_2^{ed} \equiv y_1^d y_2^d \equiv (y_1y_2)^d \pmod N$.

**12. Proof: modular arithmetic.**

A prime number $p$ is called a *Mersenne prime* if it is one less than a power of two. In other words, it is in the form $2^n - 1$ for some integer $n \geq 2$.

1. For Mersenne prime $p = 2^n - 1$, what is the smallest natural number congruent to $2^n \pmod p$?
2. For any positive integer $a$, what is the smallest natural number congruent to $(2^a)^n \pmod p$?
3. (5 points) Using the previous parts, prove that there are at least $n$ distinct values of $x \pmod p$ such that $x^n \equiv 1 \pmod p$.

**Answer:**

1. 1. $x \equiv 2^n \pmod p \implies x \equiv 2^n \equiv 1 \pmod{2^n - 1}$, so $x = 1$ works.
2. 1. $(2^a)^n \equiv (2^n)^a \equiv 1^a \pmod p$.
3. In part (b) we've already proved that $(2^a)^n \equiv 1 \pmod p$. We also proved in part (a) that $2^n \equiv 1 \pmod p$, so non-congruent values of $x$ range from $2^0$ to $2^{n-1}$, yielding $n$ values. If we take $a = 0, 1, \ldots, n-1$, then we see $n$ values that provide a working construction.

**13. Polynomials.**

1. Give an expression for a polynomial under arithmetic modulo 7 that passes through $(1,0)$ and $(2,5)$.
   **Answer:** $5x + 2 \pmod 7$. One can fit the polynomial or see that it is a line with slope 5 and then find the intercept.
2. Given that you are working over arithmetic modulo a prime $p$, how many polynomials of degree at most $d$ pass through a given $d-1$ points? (Assume $p$ is much larger than $d$. Answer possibly in terms of $p$ and $d$.)
   **Answer:** $p^2$. One can choose 2 more $x$-values and assign any of $p$ values for those to produce two more points. Each corresponds uniquely to a different polynomial.
3. The Lagrange interpolation scheme from the notes for $d+1$ points, $(x_1,y_1), \ldots, (x_{d+1}, y_{d+1})$, defines the polynomials $\Delta_1(x), \ldots, \Delta_{d+1}(x)$.

   (a) How many roots does $\Delta_1(x)$ have? (Possibly in terms of $d$, or state "Unknown" if there is insufficient information.)
   **Answer:** $d$. By construction we have a factor of d factors of the form $x - x_j$ for $j \neq 1$

   (b) Consider the polynomial $P(x) = \Delta_1(x)\Delta_2(x)$.

      i. What is the degree of $P(x)$? (Possibly in terms of $d$, or state "Unknown" if there is insufficient information.)
      **Answer:** $2d$. The product of two degree $d$ polynomials is of degree $2d$.

ii. How many values of $x$ are there where $P(x) = 0$? (If the number of values can vary, answer "Unknown", otherwise provide a number or expression possibly in terms of $d$.)
**Answer:** $d+1$. The polynomials have factors of $(x-x_i)$ for all the $d+1$ points that are given. They also have no other zeros as if they did they would have $x-r$ as a factor.

(c) True or false: Every polynomial of degree $d$ over the reals has exactly $d$ real roots.
**Answer:** False. $x^2+x+1$ has degree 2 but has no roots.

**14. Polynomial: applications.**

1. Consider a channel that has at most $e$ erasure errors and $k$ corruptions. How many packets should one send to ensure that an $n$ packet message can be recovered?
   **Answer:** $n+2k+e$. You may receive only $n+2k$ packets and can tolerate $k$ errors if you do.
2. Consider the Berlekamp-Welch error correction scheme where the error polynomial is $E(x) = x^2 - 1 \pmod{13}$. Where are the errors? That is, for which $x$-values do you have $P(x) \neq r_x$? (Answer should be a list of value(s) from $\{0,1,\ldots,12\}$.)
   **Answer:** At $x = 1$ and $x = 12$. $(x^2-1) = (x+1)(x-1) \pmod{13}$ so $x$ has roots at 1 and $-1 \pmod{13}$.
3. Consider using the polynomial scheme from class to share the secret number 5 with 10 people such that any 3 people can recover the secret. What is the smallest modulus that one can work in?
   **Answer:** 11. You need at least 10 points other than the value at 0 to share the secret when the value is encoded in $P(0)$ and the modulus needs to be prime.
4. (5 points) Describe a secret-sharing scheme in which two groups of 5 and 7 people can retrieve the secret when there is at least a majority of both groups present.
   **Answer:** Have a polynomial of degree 2 and a polynomial of degree 3 for the two groups where the secrets revealed by each group are points on a degree 1 (master) polynomial. One can recover a master polynomial (line) with two points which are the "secrets" for the two "group polynomials which can be recovered by a majority of the people in each group.
   The modulus for the group of 5 could be 7 and the modulus for the group of 7 could be 11.

**15. Computability/Countability.**

1. The set of all finite subsets of a countably infinite set is uncountable.
   **Answer:** False. Any countable set has a bijection with the naturals, and one can list the subsets in order of the sum of their values. Every finite subset has a finite sum and therefore will appear in the listing.
2. The set of all subsets of a countably infinite set is uncountable.
   **Answer:** True. Assume the sets are countable and thus each set corresponds to a natural number: $S_i$. The set $\{i | i \not\in S_i\}$ cannot be any of the $S_i$'s since it differs on whether $i$ is in the set of not.
3. A real number is computable if there is a program $P(n)$ that runs in finite time that computes the $n$th digit of the number.
   (a) True or false: Every real number is computable.
   **Answer:** False
   (b) (5 points) Prove or disprove the statement from part (a).
   **Answer:** The set of programs is countable but the real numbers are not, therefore there must be a real number that is not computable. In fact, the number of uncomputable real numbers is uncountable.

**16. Counting.**

You may leave your answer as an expression using factorial notation, e.g., $n!$, or the choose notation, e.g., $\binom{n}{k}$, unless otherwise specified.

1. How many permutations of the word ABRACADABRA are there?
   **Answer:** $\frac{11!}{5!2!2!}$. 11 letters gives the numerator, 5 A's, 2 B's, 2' R's to divide out for orderings.
2. How many ways are there to form a string with exactly 4 A's and 3 B's?
   **Answer:** $\binom{7}{3}$. Choose positions for 3 $B$'s out of 7 positions.
3. How many ways are there to split $n_1$ indistinguishable apples and $n_2$ indistinguishable bananas among $k$ people? (An expression possibly involving $n_1$, $n_2$ and $k$.)
   **Answer:** $\binom{n_1+k-1}{k-1}\binom{n_2+k-1}{k-1}$.
4. You have a drunken sailor walking along the real line starting at 0 and ending at $n$ and the sailor takes steps forward or backward of size 1. The sailor uses $n+2k$ steps in total. How many possible ways could this happen? For example, for $n=2$ and $k=1$, one of the possible ways is "backward, forward, forward, forward" or "forward,forward,forward,backward". (Note that the sailor went below 0 in the first example and past 2 in the second which is allowed.)
   **Answer:** $\binom{n+2k}{k}$. Let $f$ ($b$) be the number of forward (backward) steps. We have $f+b=n+2k$ and $f-b=n$, which means $f=n+k$ and $b=k$, so we need to choose $k$ places in the sequence of $n+2k$ steps to go backwards.
5. Let $S_n$ be the number of ways to add up 1's and 2's to obtain $n$, where order matters. (For example, $S_3=3$, with the possible ways being $1+1+1$, $1+2$ and $2+1$.)
   (a) Give an expression involving a summation for $S_n$. (Hint: consider summing over cases.)
   **Answer:** $S_n=\sum_{i=0}^{\lfloor n/2\rfloor}\binom{n-i}{i}$. Each term counts the number of ways to arrange $i$ 2's and $n-i$ 1's
   (b) Give a recursive expression for $S_n$ for $n\geq 2$. (You may assume that $S_0=1$, and $S_1=1$.)
   **Answer:** $S_n=S_{n-1}+S_{n-2}$. This follows from the fact that you have $S_{n-1}$ ways where 1 is the first term and you have $S_{n-2}$ ways where 2 is the first term.