CS 70 Discrete Mathematics and Probability Theory
Fall 2024 Hug, 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) What is the conjunction of **all** student answers for this question?

Answer: False. As long as one student answers False, then the conjunction will become False.

3. Propositional Logic

1. Consider the following statements, and determine whether they are *always true*, regardless of the values of the propositions P and Q.
   If the statement is always true, answer "Yes", and if the statement is not always true, answer "No".
   (a) $\neg$True
   Answer: No, this statement is always false. The negation of true is false.
   (b) $P \vee [(P \implies Q) \wedge (P \implies \neg Q)]$
   Answer: Yes, this statement is always true. If P is true, the statement holds, other P is false and False implies both true and false.
   (c) $\neg(P \implies Q) \equiv (P \wedge \neg Q)$
   Answer: Yes. This is De Morgan's law applied to $\neg P \vee Q$ which is equivalent to $P \implies Q$.
2. Consider the following implication, for a non-empty universe S:
$$\big[(\forall y \in S)(\exists x \in S)\big(Q(x) \wedge P(y)\big)\big] \implies \big[\big((\exists x \in S)Q(x)\big) \wedge \big((\forall y \in S)P(y)\big)\big]$$
   (a) Is the implication always true, regardless of the choice of predicates $P(\cdot)$ and $Q(\cdot)$?
   Answer: Yes.
   (b) Justify your answer, through either a counterexample or a brief explanation.
   Answer: Intuitively, this is because $Q(x)$ is only dependent on x, while $P(y)$ is only dependent on y. This means that we can safely move the $\forall y$ to only apply to $P(y)$, and we can safely move the $\exists x$ to only apply to $Q(x)$.
   Formally, we have
$$\begin{aligned}(\forall y \in S)(\exists x \in S)\big(Q(x) \wedge P(y)\big) &\implies (\forall y \in S)\big((\exists x \in S)Q(x) \wedge (\exists x \in S)P(y)\big)\\ &\equiv (\forall y \in S)\big((\exists x \in S)Q(x) \wedge P(y)\big)\\ &\equiv (\forall y \in S)(\exists x \in S)Q(x) \wedge (\forall y \in S)P(y)\\ &\equiv (\exists x \in S)Q(x) \wedge (\forall y \in S)P(y)\end{aligned}$$

(Note here that although we cannot always distribute $\exists$ over $\wedge$, the implication still holds.)

4. Proofs

1. (10 points) Let $n > 4$ be a composite number. Prove that

$$n \mid (n-1)!$$

Hint: Consider the cases when n is and is not a perfect square.

Answer: Since n is composite, there exists a, b such that $n = ab$ and $1 \leq a, b \leq n-1$.

- If $a \neq b$, then a, b are two distinct numbers in the sequence $1, 2, ..., n-1$. Hence $n = ab$ divides $(n-1)!$
- If $a = b$, then since $n = a^2 > 4$, we have $a > 2$ and consequently $2a < a^2 = n$. This means that $a, 2a$ are two distinct numbers in the sequence $1, 2, ..., n-1$, which implies that $2a^2 = 2n$ divides $(n-1)!$.

Note that for the case when n is not a perfect square, it is not correct to state that all the factors of n are contained in the factorial. Consider the example where $n = 18 = 3^2 \cdot 2$. The number 3 only appears once in the factorial, we would have to use logic similar to the perfect square case to justify why the other 3 exists as a factor of another number in the factorial.

2. (6 points) Prove that for $r \in \mathbb{R}$, if r^2 is irrational, then r is irrational.

Answer: The contrapositive is the statement: "if r is rational, then r^2 is rational." Since r is rational, we can write $r = a/b$ for $a, b \in \mathbb{Z}$ and $b \neq 0$. This means that $r^2 = a^2/b^2$. Since a^2 and b^2 are still integers with $b \neq 0$, we can conclude that r^2 is rational.

5. Induction.

(12 points) Prove that $7 \mid \left(3^{(2n+1)} + 2^{(n-1)}\right)$ for $n \geq 1$ by induction. That is, you should have a clear base case, induction hypothesis, and induction step.

Answer: Base Case: $n = 1$. $3^3 + 1 = 28 = 4 \times 7$.

Induction Hypothesis: Suppose that for a fixed but arbitrary n, we have $3^{2n+1} + 2^{n-1} = 7k$ for some integer k.

Induction Step: We'd like to show that $3^{2(n+1)+1} + 2^{(n+1)-1} = 7\ell$ for some integer ℓ.

$$\begin{aligned}
3^{2(n+1)+1} + 2^{(n+1)-1} &= 3^{(2n+1)+2} + 2^{(n-1)+1} \\
&= 9 \times 3^{2n+1} + 2 \times 2^{n-1} \\
&= 7 \times 3^{2n+1} + 2(3^{2n+1} + 2^{n-1}) \\
&= 7 \times 3^{2n+1} + 2(7k) && \text{(by IH)} \\
&= 7(3^{2n+1} + 2k)
\end{aligned}$$

Since $(3^{(2n+1)} + 2k)$ is an integer, we have completed the proof.

6. Stable Matchings.

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

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

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

(a) (3 points) Describe the job optimal pairing for this instance.

A: B: C:

Answer: $(A,1)(B,3),(C,2)$. C has to be with 2, since they are each other's favorite. The job-optimal matching pairs A and B with their favorites out of the candidates that are left.

(b) (3 points) Describe the candidate optimal pairing for this instance.

A: B: C:

Answer: $(A,3)(B,1),(C,2)$. C has to be with 2, since they are each other's favorite. The candidate-optimal matching pairs 1 and 2 with their favorites out of the jobs that are left.

(c) (3 points) Describe another stable pairing for this instance that is neither job optimal nor candidate optimal, or indicate that there is none.

OR A: B: C:

Answer: None. Since C has to be with 2, there are only two possible pairings left, the ones we reported above.

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

2. If a job is paired with its least preferred candidate in the job optimal matching, then it is the least preferred job for every candidate.

   Answer: False. It is simply less favored than whoever every other candidate is paired with. For example, consider the following set of preference lists:

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

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

   Here, since $(A,1)$ and $(B,2)$ are at the top of each other's preference lists, they must be paired together in any stable matching. This means that $(C,3)$ necessarily needs to be paired together, and thus C is paired with its least preferred candidate in the job optimal matching (the only matching), but C is not the least preferred job for every candidate.

3. If a job is paired with the same candidate in every stable matching, then that candidate is at the top of the job's preference list.

   Answer: False. In the example from the previous part, we see that there is only one stable pairing, and job C is always paired with candidate 3, which is not at the top of its preference list.

4. Recall that in a given day of the propose and reject algorithm with jobs proposing, candidates keep their best job offer on a string, and reject the rest. If a given candidate instead rejects all of their job offers on a given day (keeping none on a string), then the resulting matching (if there is one) will *always* be worse for this candidate.

   Answer: False. Consider the following preference lists.

Jobs	Preferences
A	$1 > 2$
B	$2 > 1$

Candidates	Preferences
1	$B > A$
2	$A > B$

If the candidates reject the proposals on the first day, then the resulting proposals form a candidate optimal matching.

5. If a job and candidate are paired in both the job optimal and candidate optimal matchings, then they are paired in every stable matching.

   Answer: True. The least preferred job that the candidate C can be paired with is the job in the job optimal pairing (since the job optimal pairing is the candidate pessimal pairing), and thus if it is paired to that job in the candidate optimal stable pairing as well, then this job is C's most preferred and least preferred partner in any possible stable pairing - thus C can only be paired with this job in any possible stable pairing.

7. Graphs

All graphs are simple and undirected unless otherwise specified.

1. Consider a graph G with m edges and n vertices.

   (a) If $m \geq n-1$, then G must be connected.
   Answer: False. One can have a four vertex graph, consisting of a triangle and an isolated vertex.

   (b) If $m \leq n-1$, then G must be acyclic.
   Answer: False. Same example as above.

   (c) If G is K_n, what is m in terms of n?
   Answer: $\binom{n}{2}$. This is the number of edges in a complete graph.

   (d) If G is a hypercube, what is m in terms of n? (You may find $\log_2 n$ to be useful in your expression.)
   Answer: $\frac{n \log n}{2}$. A degree-d hypercube has 2^d vertices, so equating $n = 2^d$ implies that $d = \log_2 d$. Every vertex in a degree-d hypercube has degree d, so by the Handshaking lemma, $m = \sum_{i=1}^{n} \deg(v_i)/2 = n \log_2 n/2$.

   (e) If an Eulerian tour exists in G, then m must be even.
   Answer: False. A triangle has an Eulerian tour but $m = 3$.

   (f) What is the minimum number of connected components in G? (Possibly in terms of m and/or n.)
   Answer: $\max(1, n-m)$. Suppose we start with a completely disconnected graph, with n isolated vertices. We want to add m edges to this graph, while minimizing the number of connected components. This means that every single edge we add should connect to an isolated vertex, thus decreasing the number of connected components by 1 for every edge we add.
   This can either proceed until we run out of edges to add, or we halt somewhere in the middle of the process. In the former case, we have $n-m$ connected components, and in the latter case, we'd have a single connected component. This means that at minimum, we'll have $\max(1, n-m)$ connected components in the graph.

   (g) If G is acyclic and connected, then it must have at least _____ vertices of degree 1. (Give a tight bound, possibly in terms of m and/or n.)
   Answer: 2. Any acyclic graph must have at most $n-1$ edges, and thus its total degree is at most $2n-2$. Since every vertex has degree at least 1, there must be at least two vertices of degree 1.

   (h) If G is acyclic and has c connected components, then what is m, possibly in terms of n and/or c?
   Answer: $n-c$. Suppose component i has n_i vertices. Since G is acyclic, this component must be a tree and thus have $n_i - 1$ edges. So, summing over every connected component, we have $\sum_{i=1}^{c}(n_i - 1) = (\sum_{i=1}^{c} n_i) - c = n - c$.

2. The number of odd degree vertices in a graph is always even.

   Answer: True. The sum of the degrees is even, thus the number of vertices with odd degree is even.

3. A d-dimensional hypercube can be edge colored with _____ colors. (Give a tight bound, possibly in terms of d.)

   Answer: d. We can color the edges in each dimension, i.e. of the form $(****1****, ****0****)$, a separate color since they do not share endpoints.

4. An odd-length cycle can be edge colored with _____ colors. (Give a tight bound.)

   Answer: 3. For the edge from v_1 to v_2, color it red. For next edge, from v_2 to v_3, color it blue. Continue alternating between red and blue edges until we reach the last vertex v_k where k is odd. We want to connect v_k to v_1. v_1 already has a red edge going to v_2, and v_k has a blue edge going to v_{k-1}. Thus, we need a third color for this last edge.

5. For a graph with $n+1$ edges, there exists a vertex of degree at least _____. (Give a tight bound, possibly in terms of n. Your answer should be as large as possible and hold for every graph that meets the condition.)

   Answer: 3. The average degree is $2(n+1)/n = 2+2/n$, and at least one vertex must be at least average.

8. Graph proofs.

All graphs are simple and undirected unless otherwise specified.

1. (8 points) Consider a simple connected planar graph with e edges and $v > 2$ vertices. Prove that if $e < 3v-6$, then there is a face of size at least 4 (that is, there exists a face bounded by at least 4 edges). (Recall that in a simple planar graph, every face has size at least 3.)

   Answer: Suppose for contradiction that every face has size exactly 3 (the same argument can be used in a proof by contraposition). This means that $\sum_{i=1}^{f} s_i = 3f = 2e$ by counting face-edge adjacencies. Using Euler's formula, we then have $v + \frac{2}{3}e = e + 2$ or that $e = 3v-6$. However, we know that $e < 3v-6$, which is a contradiction; this means that there must be a face of size strictly larger than 3, i.e. there is a face of size at least 4.

   Alternatively, one can use a direct proof. By Euler's formula, $v+f = e+2$, so $v = e-f+2$. Plugging into the inequality, we have that $e < 3v-6 = 3(e-f+2)-6$, which rearranges to form $3f < 2e$. We also know by face-edge adjacencies that $\sum_{i=1}^{f} s_i = 2e > 3f$, so at least one of the s_i's must be strictly larger than 3, i.e. there must be some face of size at least 4.

2. (8 points) Consider a bipartite graph $G = (V,E)$ with an Eulerian Tour. Give a method to partition the edges of the graph into two graphs where every vertex has exactly half the degree, and justify your answer.

   That is, form $G_1 = (V,E_1)$ and $G_2 = (V,E_2)$, where $E_1 \cup E_2 = E$, $E_1 \cap E_2 = \emptyset$, and every vertex v has $d_1(v) = d_2(v) = d(v)/2$ where $d(v)$ is the degree of a vertex in G, and $d_i(v)$ is the degree of v in G_i.

   Answer: Traverse the tour, and place the odd numbered edges in E_1 and the even ones in E_2.

   Since the graph is bipartite, the tour will enter one side in odd steps, and the other in even steps, so E_1 is the entering edges for one side (and leaving for the other), and E_2 is the leaving for one side (and entering for the other side.) The number of entering and leaving edges for each vertex is the same, thus each vertex has half the degree in G_1 and G_2.

   Note that the bipartite condition must be used since the algorithm fails on a triangle, which is Eulerian.

9. Modular Proofs.

1. Consider the statement: For integers a,x,y, if $\gcd(x,y) = 1$ and $a \mid xy$, then $a \mid x$ or $a \mid y$.

(a) Indicate whether the statement is true or false.
Answer: False.

(b) Justify your answer by providing a proof or a counterexample.
Answer: Consider $x = 9$ and $y = 4$ and $a = 6$. Here, $6 \mid 36$ but $6 \nmid 9$ and $6 \nmid 4$.

2. Consider $N = pqr$ for distinct primes p, q and r.

(a) What is the number of solutions to $qx \equiv 0 \pmod{N}$?
Answer: $q = N/pr$.
We can write the equation as $qx \equiv 0 \pmod{N} \implies qx = pqr \cdot k$ for some $k \in \mathbb{Z}$. Simplifying, this means that $x = pr \cdot k$ for $k \in \mathbb{Z}$.
As such, the set $\{0(pr), 1(pr), 2(pr), \ldots (q-1)(pr)\}$ are the only solutions in $\{0, 1, \ldots, N-1\}$, i.e. we can set $k \in \{0, 1, \ldots, q-1\}$.

(b) What is $x^{(p-1)(q-1)(r-1)} \pmod{N}$, if $\gcd(x, N) = 1$?
Answer: 1. See next answer.

(c) (6 points) Use the Chinese Remainder Theorem and Fermat's Little Theorem to prove that your answer to the previous part is correct.
Answer: $x^{(p-1)} = 1 \pmod{p}, x^{(q-1)} = 1 \pmod{q}, x^{(r-1)} = 1 \pmod{r}$ by Fermat's. This, implies that $x^{(p-1)(q-1)(r-1)} = 1^{(q-1)(r-1)} = 1 \pmod{p}$, and $x^{(p-1)(q-1)(r-1)} = 1^{(p-1)(r-1)} = 1 \pmod{q}$, and $x^{(p-1)(q-1)(r-1)} = 1^{(q-1)(q-1)} = 1 \pmod{r}$. All these equations are satisfied by $y = 1 \pmod{pqr}$, and it is unique by the CRT.

10. Modular: proof

Let a and n be positive integers. If m is the smallest positive integer such that $a^m \equiv 1 \pmod{n}$, we say that a has order m under arithmetic modulo n. In notation, we write that $\text{ord}_n(a) = m$.

1. What is the order of 3 under arithmetic modulo 5?
Answer: Under modulo 5, $3^1 \equiv 3, 3^2 \equiv 4, 3^3 \equiv 2, 3^4 \equiv 1$. Thus the order of 3 under modulo 5 is 4.

2. (6 points) Let $\gcd(a, n) = 1$ and m be an integer. Prove that $a^m \equiv 1 \pmod{n}$ if and only if $\text{ord}_n(a) \mid m$.
Answer: $\Leftarrow$:
Assume that $\text{ord}_n(a) \mid m$. This means that $m = k \cdot \text{ord}_n(a)$ for some k. Therefore

$$a^m \equiv a^{k \cdot \text{ord}_n(a)} \equiv (a^{\text{ord}_n(a)})^k \equiv 1^k \equiv 1 \pmod{n}$$

$\Rightarrow$:
Assume that $a^m \equiv 1 \pmod{n}$. Let $m = q \cdot \text{ord}_n(a) + r$, where $0 \leq r < \text{ord}_n(a)$. Then

$$\begin{aligned} 1 &\equiv a^m \pmod{n} \\ &\equiv a^{q \cdot \text{ord}_n(a) + r} \pmod{n} \\ &\equiv \left(a^{\text{ord}_n(a)}\right)^q \cdot a^r \pmod{n} \\ &\equiv a^r \pmod{n} \end{aligned}$$

Since $\text{ord}_n(a)$ is the smallest positive integer that satisfies $a^x \equiv 1 \pmod{n}$, it follows that $r = 0$. This means that $m = q \cdot \text{ord}_n(a)$, or $\text{ord}_n(a) \mid m$.

3. (4 points) Prove that if p is a prime and a is an integer such that $p \nmid a$, then $\text{ord}_p(a) \mid p - 1$.
Answer: Since $p \nmid a$, we have that $\gcd(a, p) = 1$. This means that by Fermat's little theorem, we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

It follows that $\text{ord}_p(a) \mid (p-1)$ from the previous part.

4. (8 points) Prove that there are no integers $n > 1$ where $n \mid (2^n - 1)$.

   Answer: Suppose for the sake of contradiction, there exists $n > 1$ such that $n \mid 2^n - 1$. Let p be its smallest prime factor. Note that $p \neq 2$.

   - Since $p \mid n$ and $n \mid 2^n - 1$, we have $2^n \equiv 1 \pmod{p}$. From part 2, we have $\text{ord}_p(2) \mid n$.
   - From part 3, $\text{ord}_p(2) \mid p-1$, which implies that $\text{ord}_p(2) \leq p-1 < p$.

   Since n is a multiple of $\text{ord}_p(2)$ and $\text{ord}_p(2) < p$, n has a prime factor that is strictly less than p. Contradiction. Hence, such n does not exist.

11. Modular arithmetic.

In the following parts, when working under arithmetic modulo N, give your answers in the range $\{0, 1, \ldots, N-1\}$.

1. What is $7^{26} \pmod{10}$?
   Answer: $9 \pmod{10}$. For $p = 2$, $q = 5$, we have $pq = 10$ and $(p-1)(q-1) = 4$, and thus $6(p-1)(q-1)+2 = 26$, and thus, using the the fact that $7^{(p-1)(q-1)} \equiv 1 \pmod{pq}$, we have $7^{26} = 7^2\left(7^4\right)^6 \equiv 7^2 \cdot 1 \equiv 49 \equiv 9 \pmod{10}$
2. What is the multiplicative inverse of $7 \pmod{68}$?
   Answer: $39 \pmod{68}$.

$$\begin{aligned} 7(0)+68(1) &= 68 \\ 7(1)+68(0) &= 7 \\ 7(-9)+68(1) &= 5 \\ 7(10)+68(-1) &= 3 \\ 7(-29)+68(3) &= 1 \end{aligned}$$

   Check $-7 \times 29 + 68 \times 3 = -203 + 204 = 1$. Also $-29 \equiv 39 \pmod{68}$.
3. For integers $x \neq y$ and m, n with $\gcd(m,n) = d$, $x \equiv y \pmod{n}$ and $x \equiv y \pmod{m}$, then $|x-y| \geq$ _____.
   Answer: mn/d. We can rewrite the equations to say that $x - y \equiv 0 \pmod{n}$ and $x - y \equiv 0 \pmod{m}$. This means that $x - y$ must be a multiple of n and also a multiple of m. As such, $x - y$ must be a multiple of $\text{lcm}(n,m) = mn/d$, since m and n share a common factor of d. We can then conclude that any two distinct values of x and y must then differ by at least mn/d.
4. How many solutions to the equation $10x \equiv 5 \pmod{505}$ are there for $x \in \{0, 1, \ldots, 504\}$?
   Answer: 5. If $10x \equiv 5 \pmod{505}$, then $10x = 5 + 505k$ for some integer k, and dividing by 5 yields $2x = 1 + 101k$, or $2x \equiv 1 \pmod{101}$. Therefore, $x = 2^{-1} \cdot 1 \pmod{101}$, so there is a unique solution mod 101; call this solution x^*. For any integer i, $x = x^* + 101i$ is also a solution, since $10x = 10x^* + 2 \cdot 505i \equiv 10x^* \equiv 5 \pmod{505}$. For $i \in \{0, 1, 2, 3, 4\}$ these are all distinct solutions mod 505, but $x + 101 \cdot 5 \equiv x + 101 \cdot 0 \pmod{505}$, so there are 5 unique solutions mod 505.
5. Consider an RSA scheme with public key (N, e) and private key d. Recall that the encoding of a message x is $E(x) = x^e \pmod{N}$ and that the decoding is $D(y) = y^d \pmod{N}$.
   (a) $D(E(x)) \equiv E(D(x)) \pmod{N}$, for all x.
   Answer: True. Any encryption/decryption scheme (or a function and inverse) over the same range and domain yields an identity function, in either order.

(b) Give an expression that "decodes" a doubly encoded $y \equiv E(E(x)) \pmod N$. Express your answer in terms of y, possibly using $E(\cdot)$ and $D(\cdot)$.
Answer: $D(D(y))$. $D(D(y)) = ((((x^e)^e))^d)^d = x^{e^2d^2} = (x^{ed})^{ed} = x^{ed} = x \pmod N$, the second and third inequality being due to $D(E(x)) = x^{ed} = x \pmod N$.

(c) For $a \equiv x^e \pmod N$ and $b \equiv y^e \pmod N$, what is the value of $D(ab) \pmod N$? Your answer may be in terms of x and/or y.
Answer: $xy \pmod N$. $ab = (xy)^e \pmod N$, thus $D(ab) = (xy)^{ed} = xy \pmod N$.

12. Polynomials.

We say a polynomial is of degree d if it can be written in the form $a_d x^d + a_{d-1}x^{d-1} + \cdots a_0$. We say that a polynomial is of degree exactly d if $a_d \neq 0$.

1. Give a polynomial of degree 2 under GF(5) that contains the points $(0,1)$, $(1,0)$, and $(3,0)$.
Answer: $2(x-1)(x-3) \pmod 5$. This is Lagrange interpolation.

2. (3 points) Consider a polynomial of degree 2 under GF(5) that contains the points $(0,0)$, $(1,1)$, and $(2,4)$. In standard form, this polynomial can be written as $ax^2 + bx + c$. What are the coefficents of this polynomial?

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

Answer: $x^2 \pmod 5$. One can see that $a_0 = 0$ from the first point, and then one has two equations $a_2 + a_1 = 1 \pmod 5$ and $4a_2 + 2a_1 = 4 \pmod 5$. Subtracting the first from the second twice yields $2a_2 = 2$ or $a_2 = 1$. And plugging in yields $a_1 = 0$. Lagrange interpolation can be done, but its slow. One can guess as well, I suppose.

3. Given the points $(x_1,y_1),(x_2,y_2),(x_3,y_3),(x_4,y_4)$, how many polynomials of degree at most 4 pass through these four points, when working in GF(p), where $p \geq 5$ is prime? (Your answer may possibly be in terms of p.)
Answer: p. A degree 4 polynomial is determined by 5 points, 4 of which are already specified. Thus, there is only one remaining point, which can be any value in mod p.

4. Given a polynomial $P(x)$ of degree exactly d and another polynomial $D(x)$ of degree exactly $d' < d$, we can perform polynomial division to construct polynomials $Q(x)$ and $R(x)$ such that $P(x) = Q(x)D(x) + R(x)$, where the degree of $R(x)$ is as small as possible.

   (a) What is the exact degree of $Q(x)$, possibly in terms of d and d'?
   Answer: $d - d'$. The leading coefficient of x^d has to be nonzero and therefore $Q(x)$ must have degree at least $d - d'$. It is sufficient due to polynomial factoring.

   (b) Give a tight upper bound on the degree of $R(x)$, possibly in terms of d and d'.
   Answer: $d' - 1$. One is dividing $P(x)$ by $Q(x)$, and one can always eliminate the coefficient corresponding to the highest degree term of $Q(x)$ in the factoring algorithm.

13. Errors, erasures, and secrets.

1. Assume that 5 TA's have a point on a polynomial $P(x)$, and 3 professors have a point on a polynomial $Q(x)$, and there is a secret s, hidden at $P(0) = Q(0) = s$. A majority of either group should be able to reconstruct the secret. Also assume that we are working in arithmetic modulo p, where p is prime.

   (a) What should the degree of the polynomial for $P(x)$ be?
   Answer: 2. Any 3 points are sufficient to reconstruct the polynomial.

(b) What should the degree of the polynomial for $Q(x)$ be?
Answer: 1. Any 2 points are sufficient to reconstruct the polynomial.

(c) How large should the modulus p be? (Your answer may be in terms of s.)
Answer: $p \geq \max(s+1, 6)$. One has to have at least 6 points, 0 for the secret and the five point values handed to the TA's.

2. Consider a polynomial $P(x) = 2x^2 + 3x + 3 \pmod 5$, where we send $P(0), P(1), P(2), P(3)$ and $P(4)$ along a communication channel, and there was a corruption at $P(1)$.

(a) Recall that the error polynomial has the form: $E(x) = x + b_0 \pmod 5$. What is $b_0 \pmod 5$?
Answer: $4 \pmod 5$. The error polynomial is $(x-1) = x+4 \pmod 5$

(b) Recall that $Q(x) = P(x)E(x) = q_d x^d + \cdots + q_1 x + q_0$.

i. What is d, the degree of $Q(x)$?
Answer: 3. The degree of $P(x)$ plus the degree of $E(x)$.

ii. What is q_d?
Answer: $2 \pmod 5$. The product of the leading coefficients of $E(x)$ and $P(x)$.

iii. What is q_0, in terms of b_0?
Answer: $3b_0 = 2 \pmod 5$. The product of the trailing coefficients of $E(x)$ which is $b = 4 \pmod 5$ and $P(x)$ which is $3 \pmod 5$.

14. Polynomials, and Roots, and Counting

All polynomials below are over GF(p). We say a polynomial is of degree d if it can be written in the form $a_d x^d + a_{d-1}x^{d-1} + \cdots a_0$. We say that a polynomial is of degree exactly d if $a_d \neq 0$.

In the following parts, you may leave your answers unsimplified (i.e. you can leave binomial coefficients, factorials, exponents, etc. as is), but you may not use any summation or product notation (i.e. you may not use $\sum$ or $\prod$).

1. How many polynomials of degree exactly d over arithmetic modulo a prime p are there?
Answer: $(p-1)p^d$. There are $p-1$ possible values for the leading coefficient and p possible values for the d others coefficients. Use the first rule of counting.

2. Any polynomial of degree exactly 1 has exactly 1 root.
Answer: True. Any degree 1 polynomial has $mx+b$, where $m \neq 0$, thus there is a root at $-m^{-1}b$.

3. Give a quadratic polynomial with a root at $x = 1$ and nowhere else.
Answer: $(x-1)^2 \pmod p$. Plugging in $x = 1$ yields zero, otherwise it is the square of a non-zero number which is zero.

4. How many polynomials are there of the form: $a(x-r)^2$, where a is nonzero?
Answer: $(p-1)p$. $(p-1)$ possibilities for a, and p possibilities for r.

5. How many polynomials are there of the form: $a(x-r_1)(x-r_2)$ with $r_1 \neq r_2$, where a is nonzero? (Note that $(x-1)(x-2)$ is the same polynomial as $(x-2)(x-1)$.)
Answer: $(p-1)\binom{p}{2}$. $(p-1)$ possibilities for a, and $\binom{p}{2}$ possible pairs for r_1 and r_2.

6. How many polynomials of degree exactly 2 have 0 roots?
Answer: $(p-1)(p^2 - \binom{p}{2} - p)$. There are $(p-1)p^2$ polynomials of degree 2, and we subtract the polynomials with exactly 1 or exactly 2 roots.

7. Given k fixed constants $r_1, \ldots, r_k$, how many polynomials are there of the form:

$$(x-r_1)^{b_1}(x-r_2)^{b_2}\cdots(x-r_k)^{b_k}$$

$b_i \geq 1$ and $\sum_{i=1}^{k} b_k = d$, where $d \geq k$ is a given constant?
Answer: $\binom{d-1}{k-1}$. Recall b_i is the number of terms for each root r_i but with the restriction $b_i \geq 1$, thus think of each root already having 1 "star" assigned, and the rest are free to be distributed to any b_i. The total number of "stars" that we can distribute is thus $d-k$. The number of "bars" is the k, the number of roots. Thus, we have $\binom{d-k+(k-1)}{k-1} = \binom{d-1}{k-1}$.

15. 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. A bridge game has 4 players who each get 13 cards, and each set of 13 cards is considered a bridge hand. Assume that we are working with a standard deck of cards, which has 52 cards in total.
   (a) How many 13 card bridge hands are there? (The order of cards in a hand does not matter.)
   Answer: $\binom{52}{13}$. Choosing 13 cards from 52.
   (b) How many ways can the 52 cards be split among the four players? (That is, players 1 through 4 each get a different hand of 13 cards, and each card is in exactly one player's hand.)
   Answer: $\binom{52}{13}\binom{39}{13}\binom{26}{13}\binom{13}{13}$. Choosing 13 cards from 52. Then 39 cards are left, so choose 13 from 39 for the second player. Similarly, 26 cards are left after 2 players get a bridge hand, so choose 13 from 26 for the third player. The last player gets the final 13 cards, and $\binom{13}{13} = 1$.
2. How many solutions to $x_1 + \cdots + x_k = n$ are there, where each $x_i \geq -1$ and is an integer?
   Answer: $\binom{n+2k-1}{k-1}$. One can construct a solution using k non-negative integers that add up to $n+k$ and then subtract 1 from each. Thus, it is the number of ways to find k numbers that add up to $n+k$.
3. Consider the following sequence of letters: CANTSTANFURD
   (a) How many ways can you rearrange the letters in CANTSTANFURD? (That is, how many anagrams are there?)
   Answer: $\frac{12!}{2!2!2!}$. 12 characters, 2 A's, 2 N's, 2 T's, and one C, S, F, U, R and D.
   (b) Let x be the answer to part (a). How many orderings of the letters are there such that C is before S, and S is before D? Note that C, S, and D are not necessarily adjacent to each other. Express your answer in terms of x.
   Answer: $\frac{x}{3!}$. There are 3! orderings of C, S and D, and only 1 is allowed.
   (c) Let x be the answer to part (a). How many orderings of the letters are there such that both A's are before the S? Note that the A's are not necessarily adjacent to the S or to each other. Express your answer in terms of x.
   Answer: $\frac{x}{3}$. There are $\binom{3}{1}$ orderings of two A's and S, and only 1 is allowed.
4. How many binary strings of length n are there with k ones?
   Answer: $\binom{n}{k}$. Choose k places out of n to be 1.
5. How many ways are there to split five identical \$1 dollar bills among 4 head TA's?
   Answer: $\binom{8}{3}$. 5 stars and 3 bars to split the dollars, before the first bar are Alec's stars, before the second are Evelyn's, and then Gavin's, and finally Joshua gets the last group.