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 have any other browsers open while 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.

Signed: _____

(Rewritten by Alec Li, as the original solutions have mistakes and unclear answers.)

2 Warmup, Propositions, Proofs

1. $\neg(P \implies Q) \equiv (P \wedge \neg Q)$

● **True** ○ False

Answer: Since $P \implies Q \equiv \neg P \vee Q$, we can use DeMorgan's law to simplify $\neg(\neg P \vee Q) \equiv P \wedge \neg Q$.

2. $\forall x \in S,\ (Q(x) \vee P(x)) \equiv (\forall x \in S,\ Q(x)) \vee (\forall x \in S,\ P(x))$

○ True ● **False**

Answer: One such counterexample is to take $S = \mathbb{N}$, the set of natural numbers, and let $P(x) =$ "x is even", $Q(x) =$ "x is odd". It is always true that any natural number is either even or odd, but it is not true that *every* natural number is even, or that *every* natural number is odd.

3. $(\exists x \forall y,\ Q(x,y) \wedge P(x)) \implies \exists x,\ P(x)$

● **True** ○ False

Answer: Since there exists an x where $Q(x,y)$ and $P(x)$ are both true, there must be an x such that $P(x)$ alone is true (just take the same x's).

4. $(\exists x \forall y,\ Q(x,y) \vee P(x)) \implies \exists x,\ P(x)$

○ True ● **False**

Answer: The difference in this part compared to the previous is now we aren't guaranteed that $P(x)$ is always satisfied on the LHS; $P(x)$ could always be false, and $Q(x,y)$ could always be true.

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

● **True** ○ False

Answer: This is just the statement of the principle of induction; $P(0)$ is the base case, and $(\forall n \in \mathbb{N},\ P(n) \implies P(n+1))$ is the inductive step. The RHS is equivalent to $\forall n \in \mathbb{N},\ P(n)$ if we distribute the negation, which is indeed the inductive claim.

6. **More Cards to Flip?** Your friend states that "All plants that are shipped to a Californian address must have originated in California." Staying indoors with windows closed all day, you are suddenly intrigued by this rule.

Which of the following would you do to test (falsify) your friend's statement?

(a) Find the destination of Megan's English Ivy plant, being shipped from Oregon

(b) Find the destination of Tyler's Rubber Tree plant, being shipped from California

(c) Find the origin of Albert's Aloe Vera plant, who received it in California

(d) Find the origin of Lili's Bamboo Palm plant, who received it in Seattle

(Answer may include more than one.)

(a) and (c)

Answer: An English Ivy shipped from Oregon, if shipped to California, would break the rule—this would be a plant shipped to California that did not originate from California.

A Rubber Tree shipped from California, if shipped anywhere, would never break the rule—if it was shipped to California, it would satisfy the rule, and if it was shipped anywhere else, the hypothesis of the rule would be false (it's a vacuous truth).

An Aloe Vera shipped to California, if shipped from elsewhere, would break the rule—this would be a plant shipped to California that did not originate from California.

A Bamboo Palm plant shipped to Seattle, if shipped from anywhere, would never break the rule—the hypothesis is false (it's a vacuous truth).

7. If n and m have the same prime factorizations, then they are the same number.

● **True** ○ False

Answer: We can just multiply the prime factorizations and we'd get the same number.

8. If $xy = n$ and $uv = n$, with $x < y$ and $u < v$, then $x = u$ and $y = v$.

○ True ● **False**

Answer: Take $n = 30$. We can have $x = 2$, $y = 15$, where $xy = 30 = n$, and we can also have $u = 5$, $v = 6$, where $uv = 30 = n$ as well.

9. If $d \mid x$ and $d \mid (x + 2y)$, then $d \mid y$.

○ True ● **False**

Answer: Suppose $d = 2$, $x = 2$, and $y = 1$. It is true that 2 divides $x = 2$ and $x + 2y = 2 + 2 \cdot 1 = 4$, but 2 does not divide y.

3 Stable Matchings

In the following, consider a stable matching instance with n candidates and n jobs each with complete preference lists.

1. The only stable pairing in any instance is produced by the job propose and candidate reject algorithm.

○ True ● **False**

Answer: There could be many stable matchings; the propose-and-reject algorithm only produces one such stable matching.

2. Any job has a unique pessimal candidate.

● **True** ○ False

Answer: The pessimal candidate is defined to be the least preferred candidate in any stable matching—there are no ties, so this candidate must be unique.

3. If a candidate rejects a job in the job propose and reject algorithm, there is *no* stable pairing where that candidate and job are paired.

● **True** ○ False

Answer: The propose-and-reject algorithm is job optimal; there exists no stable matching where any job gets a more preferred candidate. This means that if a job is rejected, there can be no stable matching between the job and the corresponding candidate.

4. Consider any stable matching instance, and a run of the job propose and candidate reject algorithm, where exactly one candidate c misbehaves. In particular, c rejects some job j falsely (that is, rejects a job j for a job j' that c prefers less). In this scenario, c is the only candidate that can be in a rogue couple in the final pairing.

● **True** ○ False

Answer: Suppose (j'', c') is a rogue couple. The improvement lemma holds for c' (as long as $c' \neq c$), which means that j'' would have asked c' prior to whomever j'' ends up with, and as such c' would not have rejected them; c' would only reject them if $c' = c$.

5. There is no stable pairing where every job is paired with its least preferred candidate.

○ True ● **False**

Answer: Suppose we have

job	preferences	candidate	preferences
A	$1 > 2$	1	$B > A$
B	$2 > 1$	2	$A > B$

The matching $(A,2),(B,1)$ is stable, as the candidates have their favorite preferences; however, both jobs have their least preferred candidate.

4 Graphs

All graphs are simple in this problem, unless otherwise stated.

1. Any tree is bipartite.

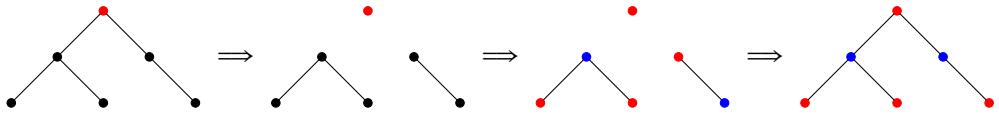
● **True** ○ False

Answer: There are a few ways to show that this is true; the main idea is that a graph is bipartite if and only if it can be 2-colored (each color corresponds to a group in the bipartite graph).

Most intuitively, we can pick an arbitrary vertex and color it one color (say red). We'd then color all neighboring vertices the second color (say blue), and continue this process, alternating colors. We'll never run into any conflicts, because trees do not contain any cycles.

More rigorously, we can argue by strong induction (briefly described here). We can split up the tree into subtrees by partitioning around an arbitrary vertex, and color each subtree recursively. That is, we pick any arbitrary vertex, color it one color, and remove all edges incident to this vertex. This leaves us with multiple disconnected subtrees, all of which can be 2-colored by the inductive hypothesis. Adding back the removed edges, we can resolve any conflicts by simply flipping the colors in the conflicting subtrees.

Here's an example of such a process:



Notice that in the last step, the right subtree had a conflicting coloring, so we flipped all the colors in the subtree to make a valid coloring. This last graph also serves as a nice visual for the first intuitive reasoning; nodes at each depth of the tree are colored a different color.

2. Any graph $G = (V, E)$ with $|E| \geq |V|$ is connected.

○ True ● **False**

Answer: Consider a graph with two disjoint cycles; for example, two triangles. We have $|E| = |V| = 6$, but the graph is disconnected.

3. Every graph that is vertex-colorable with d colors has max degree $d-1$.

○ True ● **False**

Answer: Consider a bipartite graph; any bipartite graph is 2-colorable, with no restriction on the maximum degree (i.e. the maximum degree certainly is not limited to $2-1=1$).

4. Any cycle can be edge colored with 2 colors. (Recall edge coloring is a coloring of edges so that any pair of edges incident to the same vertex have different colors.)

○ True ● **False**

Answer: Consider a cycle of length 3—a triangle. This graph cannot be edge colored with 2 colors, because the third edge will always be conflicting; this graph needs three colors.

5. For a graph G, consider a walk which contains any edge at most once and contains all the edges incident to each of its two distinct endpoints, u and v. Recall that a walk is a sequence of edges where successive edges share an endpoint, thus this walk does not reuse edges but does use all the edges incident to u and v.

   If the endpoints u and v are different:

   (a) Their degrees must be the same.

   (b) Each must have even degree.

   (c) Each must have odd degree.

   (d) The sum of the degrees of the two vertices is even.

   Answer all that are true.

   (c) and (d)

   Answer: If the walk starts and ends at two *distinct* vertices, and further contains all edges incident to both endpoints, the degrees of the endpoints must be odd. This is because the walk must leave its starting vertex, and enter the ending vertex, perhaps entering and leaving several times in between. Since all entrances/exits come in pairs apart from the initial exit from u and the final entrance to v, the degrees of u and v must be odd. Since the sum of the degrees of both vertices are odd, the total degree of u and v must be even, since odd + odd = even.

   (a) may not be true; the walk could go $u \to v \to x \to v$, and as such $\deg(u) = 1$ and $\deg(v) = 3$:

   (b) also cannot be true. Suppose we look at u; if u has even degree, and the walk contains all edges incident to u, then we must enter and exit u an equal number of times. This means that we *must* also end at u, since there must be a last entrance to u to match with our first exit from u. This is impossible if the walk has two distinct endpoints.

6. Any graph with v vertices and $v-k$ edges for $k \geq 0$ and has exactly one cycle has _____ connected components.

   $k+1$

Answer: To find the number of connected components, it can be helpful to relate this graph to a tree, as a tree has exactly one connected component. Since we are given that the graph contains exactly one cycle, we can remove one edge from the cycle to eliminate the cycle from the graph. This will not change the number of connected components.

Next, we want to see how many edges we need to add in order to turn the graph into a tree. Since a tree with n vertices will always have exactly $n-1$ edges, we must add k new edges to our graph: $(v-k-1)+(k)=v-1$, keeping in mind that we had to remove one edge to eliminate the cycle earlier.

Since each edge must connect two different components together, each new edge reduces the number of components by 1. This means that we removed k components and ended up with 1 component, so we originally had $k+1$ components.

7. There is a *simple* graph with average degree of exactly 2 that has no cycles. (Recall that simple means there is at most one edge between any pair of nodes.)

○ True ● **False**

Answer: Suppose the graph has n vertices. If the average degree is 2, then the total number of edges is

$$\frac{1}{2}\sum_{v\in V}\deg(v)=\frac{1}{2}\cdot 2n=n.$$

(This is from the handshaking lemma: $2e=\sum_{v\in V}\deg(v)$.)

In a graph with n vertices and n edges, at least one connected component has at least as many edges as vertices, and as such is a tree with some additional edges. This connected component must then have a cycle (by properties of a tree).

8. There is a directed graph, where the sum of the out-degrees *aver all vertices* is greater than the sum of in-degrees *over all vertices*.

○ True ● **False**

Answer: Every single edge contributes to one out-degree and one in-degree, so the total out-degree and in-degree over all vertices must be equal.

5 Planar graphs

Consider a connected planar graph with $v\geq 3$ vertices, and where every cycle has length at least 6.

1. Give an upper bound on the number of edges, e in terms of the number of vertices, v. (Recall, for example, that for any planar graph $e\leq 3v-6$. Your upper bound should be as tight as possible.)

$$\frac{3v-6}{2}$$

Answer: Since each cycle has length at least 6, each face has at least 6 edges. This means that summing over all the faces,

$$2e=\sum_{i=1}^{f}s_i\geq\sum_{i=1}^{f}6=6f.$$

Plugging this into Euler's formula $v+f=e+2$, we know f is always upper bounded by $\frac{e}{3}$, so we have

$$v+\frac{e}{3}\geq e+2\implies v\geq\frac{2e}{3}+2\implies\frac{3}{2}(v-2)=\frac{3v-6}{2}\geq e.$$

2. How many colors is always sufficient to vertex color such a graph?

3

Answer: From the handshaking lemma, we have $2e = \sum_{v \in V} \deg(v)$, but from the previous part we have $2e \leq 3v - 6$. This means that the average degree of a vertex is $\frac{1}{v}\sum_{v \in V} \deg(v) \leq \frac{1}{v}(3v-6) = 3 - \frac{6}{v} < 3$.

This means that there must be some vertex of degree at most 2 (since there must be some vertex of degree < 3 to make the average < 3).

We can then proceed with an inductive argument to show that 3 colors is sufficient to vertex color such a graph (we can see that 2 is not sufficient, because we could have a cycle of length 7). In the base case, we have a graph with $v = 3$ vertices, which can always be colored with 3 colors; each vertex can be its own color. Assuming that a graph with v vertices can be 3-colored, we will show that a graph with $v+1$ vertices can also be 3-colored.

Since we know that there is a vertex of degree at most 2, let us remove this vertex along with its incident edges. This gives us a new graph with v vertices which is still planar and each cycle still has length at least 6. If removing the vertex disconnects the graph, both those properties still apply to each connected component, and we can apply strong induction to see that the graph on v vertices can be 3-colored.

Adding back the vertex we removed, in the worst case we have two edges connected to two vertices of different colors. Since we have a third color, we can always color this new vertex with the third color, thus 3-coloring the original graph on $v+1$ vertices.

6 Modular Arithmetic

1. What is $2^{11} \pmod{11}$?

$2 \pmod{11}$

Answer: By FLT, we have $2^{10} \equiv 1 \pmod{11}$, and as such $2^{11} = 2^{10} \cdot 2 \equiv 1 \cdot 2 = 2 \pmod{11}$.

2. What is $2^{25} \pmod{33}$?

$32 \pmod{33}$

Answer: We can split this up into two parts; we want to find $2^{25} \pmod 3$ and $2^{25} \pmod{11}$, and we can combine the results with CRT. We have

$$2^{25} \equiv (-1)^{25} = -1 \pmod 3.$$

Further, $2^{10} \equiv 1 \pmod{11}$ by FLT, so

$$2^{25} = 2^{20} \cdot 2^5 \equiv 2^5 = 32 \equiv -1 \pmod{11}.$$

Since $2^{25} \equiv -1 \pmod 3$ and $2^{25} \equiv -1 \pmod{11}$, we must have $2^{25} \equiv -1 \equiv 32 \pmod{33}$ by CRT as well.

Alternatively, we can recognize from RSA that $2^{20} = 2^{(11-1)(3-1)} \equiv 1 \pmod{33}$, since part of the RSA correctness proof relies on the fact that $a^{k(p-1)(q-1)} \equiv 1 \pmod{pq}$. This means that we're left with $2^{25} \equiv 2^5 = 32 \pmod{33}$.

3. $ab \equiv 0 \pmod{N}$ implies that $a \equiv 0 \pmod{N}$ or $b \equiv 0 \pmod{N}$.

○ True ● **False**

Answer: As a counterexample, take $N = 6$, with $a = 2$ and $b = 3$.

4. For primes p and q, find all values of $x \in \{1, \ldots, pq-1\}$ where $x \mid \left(a^{k(p-1)(q-1)+1} - a\right)$.

p, q, 1, perhaps also a

Answer: We know by RSA that $a^{k(p-1)(q-1)+1} \equiv a$ under both mod p and mod q; this is due to FLT:

$$a^{k(p-1)(q-1)} = \left(a^{p-1}\right)^{k(q-1)} \equiv 1 \pmod{p}$$
$$a^{k(p-1)(q-1)} = \left(a^{q-1}\right)^{k(p-1)} \equiv 1 \pmod{q}$$

This means that $a^{k(p-1)(q-1)+1} - a \equiv 0 \pmod{p}$ and $\equiv 0 \pmod{q}$. As such, both p and q must divide this quantity. Further, we could have $x = 1$, and perhaps $x = a$ as well, except for the case where $a \geq pq$; these last two were not included in the official solution.

(This isn't a particularly good question in that the desired answer is quite ambiguous, but the most important thing to take away from it is the recognition of RSA in the expression.)

5. If $a \neq 1 \pmod{N}$ and $a^{k(N-1)} \neq 1 \pmod{N}$ then N is not prime.

○ True ○ False

Answer: The answer is intended to be True, but is technically False.

By FLT, we must have $a^{p-1} \equiv 1 \pmod{p}$ for all a and for any prime p. By contradiction, if N is prime then we must have $a^{N-1} \equiv a^{k(N-1)} \equiv 1 \pmod{N}$, which is contrary to the claim. This means that N must not be prime.

The problem statement was intended to have $a \neq 0 \pmod{N}$ as well; as is, we could have $a = 0$ and N still be prime.

6. How many solutions are there to $ax = b \pmod{n}$, if $\gcd(a, n) = d$ and $\gcd(b, n) = d$?

d

Answer: One useful modular arithmetic fact to know is that if $d \mid x$, $d \mid y$, and $d \mid n$, then

$$x \equiv y \pmod{n} \implies \frac{x}{d} \equiv \frac{y}{d} \pmod{\frac{n}{d}}.$$

Here, since d is the greatest common divisor of a, b, and n, dividing through by d ensures that $\frac{a}{d}$ and $\frac{n}{d}$ have no common divisors, and thus are relatively prime. This means that

$$\frac{ax}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}} \implies x \equiv \left(\frac{a}{d}\right)^{-1} \frac{b}{d} \pmod{\frac{n}{d}}$$

and thus has exactly one solution, as $\frac{a}{d}$ is invertible mod $\frac{n}{d}$.

Since we're working under mod $\frac{n}{d}$, any $x = \left(\frac{a}{d}\right)^{-1} \frac{b}{d} + k\frac{n}{d}$ is also a solution. Put another way, we have exactly one solution in the range $x \in [0, \ldots, \frac{n}{d} - 1]$, exactly one solution in the range $x \in [\frac{n}{d}, \ldots, 2\frac{n}{d} - 1]$, etc. for d intervals up to n.

This means that under mod n, we have exactly d solutions to the equation $ax \equiv b \pmod{n}$.

7. Find $x \in \{0, \ldots, pq-1\}$ where $x = a \pmod{p}$ and $x = 0 \pmod{q}$ where p and q are prime? (Your answer may involve a, p, q, $\bmod q$, $\bmod p$, and inverses, e.g., $q^{-1} \pmod{p}$.)

$aq(q^{-1} \bmod p)$

Answer: Recall that CRT for a system of two modular equations states

$$\begin{cases} x \equiv a \pmod{p} \\ x \equiv b \pmod{q} \end{cases} \implies x \equiv aq(q^{-1} \bmod p) + bp(p^{-1} \bmod q) \pmod{pq}.$$

Here, we have $b = 0$, so we only need the first term, i.e. $x \equiv aq(q^{-1} \bmod p) \pmod{pq}$.

8. For $x, y \in \mathbb{Z}$ and $x \neq y$, what is the minimum value of $|x-y|$ if $x = y = z \pmod{p}$ and $x = y = b \pmod{q}$ for primes p and q?

pq

Answer: If we just look at x, we have a system $x \equiv a \pmod{p}$ and $x \equiv b \pmod{q}$ for primes p and q. By CRT, there exists a unique solution for $x \pmod{pq}$. The same reasoning holds for y, and in fact the two solutions must be equivalent mod pq, since both are equal to $a \pmod{p}$ and $b \pmod{q}$.

As such, $x \equiv y \pmod{pq}$, and any distinct solutions must be separated by a factor of pq. This means that the minimum value of $|x-y|$ is pq.

7 Another Proof

Another proof for RSA can be done as follows.

1. Let S be the set of numbers $\{0, \ldots, pq-1\}$ relatively prime to pq. What is $|S|$? (Recall, a and b are relatively prime if $\gcd(a,b) = 1$.)

$(p-1)(q-1)$

Answer: In order for a number to be relatively prime to pq, it must not be a multiple of p and must not be a multiple of q. These are the only two cases we need to consider, because p and q are both prime.

There are q different multiples of p (i.e. $\{0, p, 2p, \ldots, (q-1)p\}$) and p different multiples of q (i.e. $\{0, q, 2q, \ldots, (p-1)q\}$). This leaves us $pq - p - q$ numbers, but notice that we've subtracted 0 twice; adding that back, we have our final answer of $pq - p - q + 1 = (p-1)(q-1)$.

(Notice that this last calculation is exactly the principle of inclusion-exclusion.)

2. For a with $\gcd(a, pq) = 1$ and $T = \{ax \pmod{pq} \mid x \in S\}$, what is the size of T?

$(p-1)(q-1)$

Answer: Recall that the function $f(x) = ax \pmod{n}$ is a bijection for prime n and $\gcd(a,n) = 1$, since we have the inverse function $f^{-1}(x) = a^{-1}x \pmod{n}$.

In our case, this means that $f(x) = ax \pmod{pq}$ is a bijection from S to itself. In particular, we know that $f(x) = ax \pmod{pq}$ is injective, since $f(x) = f(y) \implies ax \equiv ay \pmod{pq} \implies x \equiv y \pmod{pq}$, since $\gcd(a, pq) = 1$ and $a^{-1} \pmod{pq}$ exists. Further, f is surjective, since any $y \in T$ has a pre-image $a^{-1}y = a^{-1}ax = x \in S$.

Because of this bijection, we know that T has the same size as S. Further, we can see that S and T must have the same exact elements; it's always the case that $f(x) = ax \pmod{pq}$ is coprime to pq if x is coprime to pq.

3. What is $a^{|T|} \pmod{pq}$?

1

Answer: Since we know that S and T contain the same elements, the product of all elements in S must also equal the product of all elements in T. This means that we have

$$\begin{aligned}\prod_{x\in S} x &\equiv \prod_{y\in T} y \pmod{pq}\\ &= \prod_{x\in S} ax \pmod{pq}\\ &= a^{|S|}\prod_{x\in S} x \pmod{pq}\\ 1 \equiv a^{|S|} &= a^{|T|} \pmod{pq}\end{aligned}$$

Note that we canceled out the $\prod_{x\in S} x$ on both sides in the last line since each element has an inverse mod pq.

8 Polynomials: Background

When we count roots, we mean with multiplicity unless otherwise stated. That is $Q(x) = (x-2)^2$ has two roots. Polynomials are over a field unless otherwise specified.

1. If two polynomials of degree 7 share _____ points then they must be the same (working mod 17). (Answer is the smallest integer that makes the statement true.)

8

Answer: Any degree d polynomial is uniquely defined by $d+1$ points. This means that a degree 7 polynomial is uniquely determined by 8 points, and if any two degree 7 polynomials share 8 points, they must be the same polynomial.

2. If a nonzero polynomial has d roots, it must have at least degree _____.

d

Answer: We can write the polynomial in factored form, and the d roots give us at least a degree d term in the polynomial.

3. How many roots does the polynomial $x^2 - 2 \pmod 5$ have?

0

Answer: We can just try all numbers mod 5 to check:

x	0	1	2	3	4
$f(x)$	-2	-1	2	2	4

.

4. If a polynomial has d roots, its degree is at most d.

○ True ● **False**

Answer: A simple counterexample is $f(x) = x^2 + 1$ over the reals. This polynomial has no roots, but its degree is 2.

5. Given a polynomial $Q(x) = P(x)(x-2)(x-4)$, and d is the degree of $Q(x)$, what is the degree of $P(x)$?

$d-2$

Answer: We can see that simply multiplying by $(x-2)(x-4)$ will introduce another two degrees to the polynomial, so $P(x)$ must be of degree $d-2$.

6. Given a polynomial $Q(x) = P(x)(x-2)(x-4)$, and if $P(x)$ has r roots, what is the number of roots for $Q(x)$?

$r+2$

Answer: Very similar to the previous part, multiplying by $(x-2)(x-4)$ adds two new roots (perhaps increasing the multiplicity), meaning $Q(x)$ now has $r+2$ roots.

9 Polynomials: Applications

Recall for secret sharing and error tolerance to erasures and corruptions that one works over arithmetic modulo a prime p. In each of the following situations, how big should p be? (That is, fill in the blank for $p \geq$ _____.)

1. One wishes to share a secret with b-bits among n people where any k can reconstruct the secret.

$p \geq \max(2^b, n+1)$

Answer: Since the original secret must be able to be recovered fully, we must have $p \geq 2^b$ (i.e. we need to store y-values up to 2^b)—otherwise, the modulus will destroy the secret. Further, p must be large enough so that we can have $n+1$ distinct points on the polynomial (i.e. we need at least $n+1$ different x-values to create our polynomial), one for the secret, and n to distribute.

2. One wishes to communicate a message of n packets with b bits each and wants to tolerate k erasures.

$p \geq \max(2^b, n+k)$

Answer: Each packet has b bits, meaning we have a number of size 2^b that we need to be able to recover, and as such $p \geq 2^b$ (i.e. we need to store y-values up to 2^b). Further, p must be large enough so that we can have $n+k$ distinct points on the polynomial (i.e. we need at least $n+k$ different x values to create our polynomial); this allows k packets to be erased without any loss.

3. One wishes to communicate a message of n packets with b bits each and wants to tolerate k corruptions.

$p \geq \max(2^b, n+2k)$

Answer: Again, we must be able to store numbers of magnitude up to 2^b, so $p \geq 2^b$. Further we now need at least $n+2k$ different x-values such that we can tolerate k corruptions and run Berlekamp-Welch to recover our polynomial and the secret.

10 Counting: Basics

Let $S = \{1, \ldots, n\}$.

(A) All subsets of S.

(B) The number of subsets of S of size k.

(C) The number of subsets of S of size $n-k$.

(D) The number of ways for k non-negative integers that up to n.

(E) The number of ways for k positive integers that add up to n.

For each of the expressions, indicate the letter of the option above that it corresponds to.

Provide all answers that match.

1. $\binom{n}{k}$

B and C

Answer: A subset of size k of S is an unordered collection of k elements from S; this is equivalent to choosing a set of size $n-k$ from S of elements *not* in the desired subset.

2. $\binom{n}{n-k}$

B and C

Answer: This is the same as the previous part; choosing a subset of k elements is the same as choosing a set of $n-k$ elements from S *not* in the desired subset.

3. $\binom{n-1}{k-1}$

E

Answer: This is equivalent to asking: how many possible values of $x_1, \ldots, x_k$ are there such that all $x_i > 0$ and $x_1 + x_2 + \cdots + x_k = n$?

We can rewrite this equation so that we can use stars and bars directly, by letting $x_i = y_i + 1$; this means that we have a relaxed constraint that $y_i \geq 0$:

$$(y_1 + 1) + (y_2 + 1) + \cdots + (y_k + 1) = n$$
$$y_1 + y_2 + \cdots + y_k = n - k$$

Applying stars and bars directly, we have $n-k$ total stars, with $k-1$ bars, giving us $\binom{n-1}{k-1}$.

4. $\binom{n+k-1}{k-1}$

D

Answer: This is equivalent to asking: how many possible values of $x_1, \ldots, x_k$ are there such that all $x_i \geq 0$ and $x_1 + x_2 + \cdots + x_k = n$?

Along similar lines to the end of the previous part, we have n total stars, with $k-1$ bars, giving us $\binom{n+k-1}{k-1}$.

5. 2^n

A

Answer: For each element in the set, we have two options: it is contained in the subset, or it is not contained in the subset. This means that we have a total of 2^n possible subsets of S.

As an aside, it may perhaps be easiest to look at the options first, and match each with the question, rather than the other way around—it may seem a little bit contrived and vague as to how we arrive at these explanations purely from the expression given.

11 Counting and Polynomials

Assume all polynomials are over $\pmod p$ where p is a prime and $p > d$.

Again, when we count roots, we mean with multiplicity unless otherwise stated. That is, $Q(x) = (x-2)^2$ has two roots.

1. What is the number of roots of a degree 1 polynomial $\pmod p$? (A degree one polynomial is $ax+b$, where a is non-zero.)

   1

   Answer: For a degree one polynomial, a root occurs at

   $$\begin{aligned} ax + b &\equiv 0 \pmod p \\ ax &= -b \pmod p \\ x &= -b \cdot a^{-1} \pmod p \end{aligned}$$

   Here, since p is prime and a is nonzero, $\gcd(a, p) = 1$ and $a^{-1} \pmod p$ exists. This means that there is always exactly one solution x, and thus only one root to a degree one polynomial.

2. What is the number of degree d polynomials?

   $(p-1)p^d$

   Answer: A general form of a degree d polynomial is $a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$. Of the coefficients, the leading coefficient a_d must be nonzero, so there are a total of $p-1$ possibilities for a_d. All other coefficients (i.e. the d other coefficients) can vary freely, so there are a total of p possibilities for a_0 through a_{d-1}. This gives us $(p-1)p^d$ total polynomials of degree exactly d.

   Note that while counting the zeros in the form $a(x-r_1)(x-r_2)\cdots(x-r_d)$ may give the same result, it's actually a coincidence, as polynomials with no roots or with irreducible factors are not counted.

3. What is the number of exactly degree d polynomials with d distinct roots?

   $(p-1)\binom{p}{d}$

   Answer: Here, we can't count the coefficients as with the previous part; we must count the roots, as the coefficients give us no helpful information on where the roots are—we need to ensure the roots are distinct.

   As such, considering the form $a(x-r_1)(x-r_2)\cdots(x-r_d)$, we again have $p-1$ possibilities for the leading coefficient a. In this part, we have an additional restriction on the roots—they must be distinct. This means that we must choose d of the p possibilities for the location of the roots, without replacement (we have no order here, as permuting the multiplicative factors still gives the same polynomial). This gives us $(p-1)\binom{p}{d}$ total polynomials.

4. What is the number of exactly degree d polynomials with d roots (allowing for multiplicity)?

$$\boxed{(p-1)\binom{d+p-1}{d} = (p-1)\binom{d+p-1}{p-1}}$$

Answer: Counting the roots in the form $a(x-r_1)(x-r_2)\cdots(x-r_d)$, we again have $p-1$ possibilities for the leading coefficient a. Looking at the roots, we must choose d out of p possible locations for roots, *with repetition*, and still without order (as permuting factors does not change the polynomial).

This means that we have to use stars and bars—we're seeing how many roots there are at each x value. Here, we have d stars and $p-1$ bars, meaning there are a total of $\binom{d+p-1}{d} = \binom{d+p-1}{p-1}$ possible ways to choose the d roots with multiplicity. This gives us $(p-1)\binom{p+d-1}{d} = (p-1)\binom{p+d-1}{p-1}$ total polynomials.

12 Quick(ish) Proofs

1. Prove: If $d \mid x$ and $d \mid (y+kx)$ then $d \mid y$ for any integer k.

   Answer: We know that $d \mid x$, so we can write $x = id$ for some $i \in \mathbb{Z}$. Similarly, since $d \mid (y+kx)$, we can write $y+kx = jd$ for some $j \in \mathbb{Z}$.

   Substituting the equation for x, we have

   $$\begin{aligned} y + kx &= jd \\ y &= jd - kx \\ &= jd - k(id) \\ &= d(j - ik) \end{aligned}$$

   Here, since $j - ik$ is an integer, we have that $d \mid y$.

2. Prove: If $n^2 - 6n + 5$ is even, then n is odd.

   Answer: It is easiest to prove this by contraposition; the contrapositive is: If n is even, then $n^2 - 6n + 5$ is odd.

   Assuming n is even, we can write $n = 2k$ for some $k \in \mathbb{Z}$. This means that we have

   $$n^2 - 6n + 5 = (2k)^2 - 6(2k) + 5 = 4k^2 - 12k + 5 = 4k^2 - 12k + 4 + 1 = 2(2k^2 - 6k + 2) + 1.$$

   This is in the form $2i+1$ for some $i \in \mathbb{Z}$, which means that the final expression is odd.

   We could have also used contradiction here, and the proof follows in almost exactly the same manner.

   We can also use a proof by cases; notice that $n^2 - 6n + 5$ can be factored as $(n-1)(n-5)$. Assuming this expression is even, we must have a factor of 2 in either the $(n-1)$ term or the $(n-5)$ term; that is, either $n-1$ is even, or $n-5$ is even.

   In the first case, we have $n - 1 = 2k$, which means $n = 2k+1$. In the second case, we have $n - 5 = 2k$, which means $n = 2k + 5 = 2(k+2) + 1$. In both cases, we've shown that n must be odd, as desired.

3. Prove by induction: For all positive natural numbers $n \geq 1$, $3(7^n) + 2^{(5n-3)}$ is divisible by 25.

   Answer: We proceed with a proof by induction.

   Base case: For the base case of $n = 1$, we have $3(7^1) + 2^{(5\cdot 1-3)} = 21 + 4 = 25$, which is divisible by 25.

   Inductive hypothesis: Suppose that the claim holds for $n = k$; that is, $3(7^k) + 2^{(5k-3)}$ is divisible by 25.

Inductive step: We will show that the claim holds for $n = k+1$; looking at the expression, we have

$$\begin{aligned}
3(7^{k+1}) + 2^{5(k+1)-3} &= 3 \cdot 7^{k+1} + 2^{5k+5-3} \\
&= 3 \cdot 7^{k+1} + 2^5 \cdot 2^{5k-3} \\
&= 3 \cdot 7 \cdot 7^k + 32 \cdot 2^{5k-3} \\
&= 7 \cdot 3 \cdot 7^k + (7+25) \cdot 2^{5k-3} \\
&= 7 \cdot 3 \cdot 7^k + 7 \cdot 2^{5k-3} + 25 \cdot 2^{5k-3} \\
&= 7\left(3 \cdot 7^k + 2^{5k-3}\right) + 25 \cdot 2^{5k-3}
\end{aligned}$$

Here, the first term is divisible by 25 from the inductive hypothesis, and the second term is divisible by 25 since it is of the form $25m$ for some $m \in \mathbb{Z}$. This shows that the claim holds for $n = k+1$, and thus by the principles of induction, the claim holds for all $n \in \mathbb{Z}$.

As an aside, it may seem at first that the algebraic manipulation is quite arbitrary and unmotivated—remember that the main goal in the algebraic manipulation is to rewrite the expression so that we can use the inductive hypothesis. The tricky bit is rewriting the $32 = 7 + 25$ *to do some sneaky factoring.*

13 Set Operations

For a function g, define the image of a set X to be the set $g(X) = \{y \mid y = g(x) \text{ for some } x \in X\}$.

Hint: For sets X and Y, $X = Y$ if and only if $X \subseteq Y$ and $Y \subseteq X$. To prove that $X \subseteq Y$, it is sufficient to show that $\forall x((x \in X) \implies (x \in Y))$.

Let $X \Delta Y = (X - Y) \cup (Y - X)$, where $X - Y = \{x \mid x \in X \text{ and } x \notin Y\}$.

Prove $g(X)\Delta g(Y) \subset g(X \Delta Y)$.

Answer: The question originally intended to ask to prove $g(X)\Delta g(Y) \subseteq g(X\Delta Y)$, not the strict subset.

As it is, the statement with the strict subset is false; one example is with $X = Y = \{1\}$, and $g(1) = 2$. Here, $g(X) = \{2\}$ and $g(Y) = \{2\}$, meaning $g(X)\Delta g(Y) = \varnothing$. We also have $X\Delta Y = \varnothing$, meaning $g(X\Delta Y) = \varnothing$ as well. This example gives an equality; $g(X)\Delta g(Y) = g(X\Delta Y) = \varnothing$.

We will still prove the intended statement $g(X)\Delta g(Y) \subseteq g(X\Delta Y)$. Suppose $z \in g(X)\Delta g(Y)$. We have two cases: $z \in g(X) - g(Y)$, or $z \in g(Y) - g(X)$.

In the first case, where $z \in g(X) - g(Y)$, we have $z \in g(X)$ and $z \notin g(Y)$. In particular, there exists a $w \in X$ such that $g(w) = z$, and further, $w \notin Y$ too (otherwise, we'd have $z \in g(X)$ *and* $z \in g(Y)$, which contradicts our assumptions). This means that we have $w \in X - Y$.

In the second case, where $z \in g(Y) - g(X)$, we proceed similarly; we have $z \in g(Y)$ and $z \notin g(X)$. In particular, there exists a $w \in Y$ such that $g(w) = z$, and further, $w \notin X$ too. This means that we have $w \in Y - X$.

Together, if $z \in g(X)\Delta g(Y)$, we must have $w \in (X - Y) \cup (Y - X)$, i.e. $w \in X\Delta Y$ and $g(w) = z \in g(X\Delta Y)$.

14 Edge Coloring when there is no Hotel California

1. Show that an even length cycle can be edge colored with 2 colors. (Recall edge coloring is a coloring of edges so that any pair of edges incident to the same vertex have different colors.)

   Answer: Going along the cycle, we can color every other edge the same color. This makes exactly half of the edges one color, and the other half the other color.

   More formally, we can color the edges with color $i \pmod 2$, for the ith step in the traversal. Since edges incident to the same vertex will have different values of $i \pmod 2$, the two edges will have different colors.

Recall that a bipartite graph $G = (U \cup V, E)$ where $E \subset U \times V$, i.e. there are two sets U and V and every edge consists of a vertex from U and a vertex from V. It is useful to recall (without proof) that any cycle in a bipartite graph has even length.

For the following two parts, we consider a bipartite graph, $G = (U \cup V, E)$ where every vertex has degree $d = 2^k$.

2. Show that $|U| = |V|$.

   Answer: The total number of edges incident to the set U is $|U|$ is $|U|d$, since every vertex in U has degree d. However, every single edge must be incident to U, so it must be the case that $|U|d = |E|$.

   We can apply the same argument to see that $|V|d = |E|$. Together, this means that $|U|d = |E| = |V|d$, meaning $|U| = |V|$, as desired.

3. Show that the graph can be edge colored with $d = 2^k$ colors. (Hint: a previous part has something to do with $k = 1$.)

   Answer: We will proceed by induction on k.

   In the base case, we have $k = 1$, i.e. a bipartite graph where every vertex has degree $d = 2^k = 2$. This means that the graph is just a cycle of even length, which is a case that we've already covered in the first part. As such, since any even length cycle can be colored with $d = 2$ colors, the base case follows the claim.

   Assuming that the claim holds for $d = 2^k$, we want to show that the claim also holds for $d = 2^{k+1}$.

   Suppose we have a bipartite graph where each vertex has degree $d = 2^{k+1}$. There could be multiple connected components in this graph, but each one of the connected components can be traversed with an Eulerian tour (as every single vertex has even degree). WLOG suppose the tours start and end at a vertex $u \in U$.

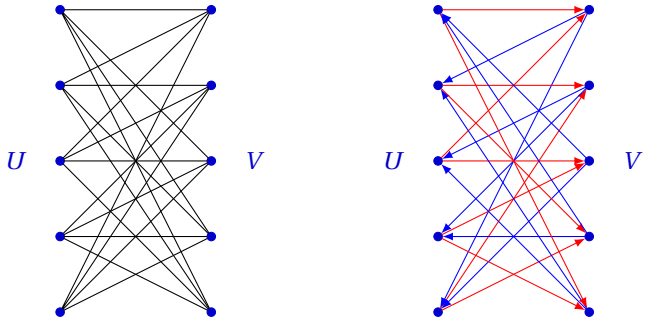
   Looking at these tours, each must have an even length (by the hint given), so we can group the edges into two groups, in the same way as we'd color an even length cycle. Notice that each of these edges in the tour must either be going into U from V, or out of U to V.

   Specifically, the first edge out of u would be in group 1, and the second edge would be in group 0 (this edge in the traversal would take us back to a vertex in U), the third edge would be in group 1, etc.

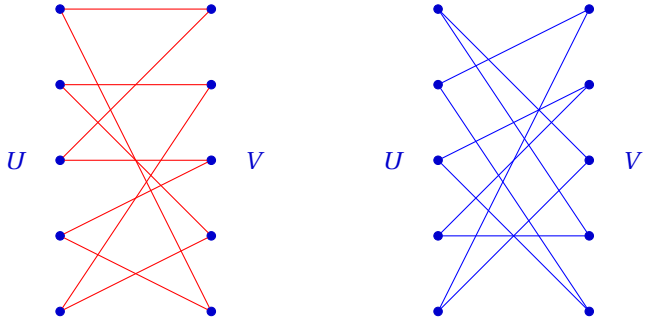
   If we look at each of the two groups individually, we can form two graphs from these two sets of edges. We know that these two graphs must each contain exactly half of the edges, and further we know that each vertex in these smaller graphs must have degree $d' = 2^k$, since we always enter and leave vertices in pairs. The two smaller graphs partition the set of edges into exactly these groups: edges leaving U and edges entering U—this partition essentially halves the degree of each vertex in the original graph.

   We can now apply the inductive hypothesis to these smaller graphs to color them with $d' = 2^k$ colors each. Combining these edges again, we've just colored the original graph with $2d' = 2^{k+1} = d$ colors, as desired.

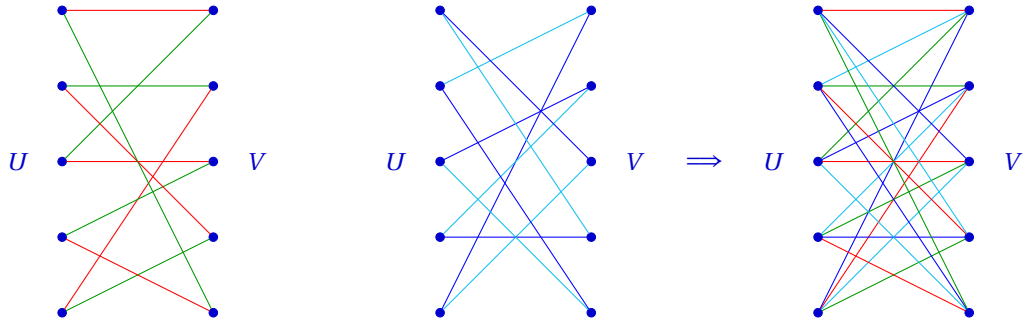
As an example, suppose we have a graph on the left, with $k = 2$, meaning each vertex has degree $d = 2^k = 4$. One possible Eulerian tour of the graph is shown on the right, with edges grouped as shown, with red in one group and blue in another group (note that these are not the actual final edge colors; the colors here just denote the groups).



If we just show the two groups individually, we have the following:



Each of these graphs now have all vertices of degree $d' = 2^{k-1} = 2$, which means that we can color them with $d' = 2$ colors from the inductive hypothesis. Putting these edges back together, we get our final colored graph with $d = 4$ colors.



The final result here may look incredibly messy and complicated, but the main thing to pay attention to is the vertices; notice that for each vertex, every single incident edge has a distinct color. This is our goal, and this process constructs such an edge coloring.