CS 70 Discrete Mathematics and Probability Theory
Spring 2021 Parekh and Rao

Midterm Solutions

PRINT Your Name: Oski Bear

SIGN Your Name: $\mathscr{OSKI}$

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 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:______________

2. Warmup, Propositions, Proofs

1. $\forall x, y \in \mathbb{R}, \exists z \in \mathbb{R}\ ((x > y) \implies x > z > y)$

   Answer: True. For every two reals, there is real that is between them.

2. $\exists z \in \mathbb{R},\ \forall x, y \in \mathbb{R}\ ((x > y) \implies x > z > y)$.

   Answer: False. There is no real that is between every pair of reals. It is true that for every pair of reals there is another real.

3. For a function $f(x)$, Consider $X = f^{-1}(A \cup B)$ and $Y = f^{-1}(A) \cup f^{-1}(B)$. (Recall that $f(X) = \{y | y = f(x) \text{ for some } x \in X\}$ and $f^{-1}(Y) = \{x | f(x) \in Y\}$.)
   Is $X \subseteq Y$, $Y \subseteq X$, or both?

   Answer: $X = Y$. If $x \in f^{-1}(A \cup B)$, then $f(x) \in A \cup B \leftrightarrow f(x) \in A$ or $f(x) \in B \leftrightarrow x \in f^{-1}(A) \cup f^{-1}(B)$.

4. If one has $n+1$ pigeons distributed into n holes, there always exist a hole with at least X pigeons. What is the largest value of X where the statement is true?

   Answer: 2. At least two pigeons must be in the same hole.

5. If $2n+1$ pigeons are placed in an n holes numbered 0 to $n-1$, there always exists a pair of holes numbered i and $i+1 \pmod n$ with a total of at least X pigeons in the two holes. What is the largest value of X where the statement is true?

   Answer: 5. If one sums the occupancy for holes i and $i+1 \pmod n$ for all the i pairs, each pigeon is counted twice, so the total of the counts is $4n+2$. Dividing by the n possibilities for i pairs, we get $4+2/n$, and thus we can conclude that the count is at least 5 for one i.

6. The equation $x^5 = 16$ has a rational solution

   Answer: False. Assume not, consider a/b with no common factors, $a^5 = 16b^5$ which implies $16 | a^5$ and $a = 2k$ for some integer k, which yields $16b^5 = (32k^5)$, and then b is even. This is a contradiction of the reduced form of the fraction a/b.

3. Stable Matchings. 2 points/part.

In the following "favorite" partner means first on preference list, "optimal" partner means the most preferred partner in any stable pairing.

1. There is a stable pairing where no job is paired with the first candidate on their list.

   Answer: True. The candidate optimal pairing in a 2 by 2 instance which is different from the job optimal pairing works. The 2 by 2 instance where jobs A, B have $1, 2$ first respectively and candidates $1, 2$ have jobs B, A respectively, is an example.

   The pairings $(A,1),(B,2)$ and $(B,1),(A,2)$ are both stable.

2. If there is a stable pairing where a job j is paired with its pessimal candidate, then all jobs are paired with their pessimal candidate in that stable pairing.

   Answer: False. Consider two instances with different optimal/pessimal pairings. Combine the instances so that entities in the other instances are later in the preference lists and one can use the optimal pairing in the first (sub)instance and the pessimal pairing in the (other).

3. No job can improve their final outcome in the jobs propose matching algorithm by submitting a false preference list.

   Answer: True. Say job j gives a fake preference list, and c is the result of the algorithm with the correct order, and c' is the result of the algorithm in the incorrect order. If c' is preferred to c then job j would have proposed to c' in the original algorithm and was rejected due to some j'. That j' would ask c' in this situation as well since their preference list remained the same, and if they were rejected from by a previous candidate, c_p, due to j who no longer asks, and since j was ultimately rejected by that previous candidate due to some j'' then j too would be rejected by that candidate due to j''. So j' would ask c' which would cause j to be rejected in this run as well.

4. No collection of jobs can conspire to improve the outcome of any job j in the jobs propose matching algorithm by jointly submitting false preference lists.

   Answer: False.

   Consider the following true preference lists, with Jobs 1,2,3 and Candidates A,B, and C.

Jobs				Candidates			
1	A	B	C	A	2	1	3
2	B	A	C	B	1	3	2
3	B	C	A	C	1	2	3

   Job 1 ends up with Candidate B, Job 2 with A, and Job 3 with C. Now see what happens when all the Jobs conspire.

Jobs				Candidates			
1	A	B	C	A	2	1	3
2	B	A	C	B	1	3	2
3	**C**	**B**	A	C	1	2	3

   Job 3 going straight for Candidate C means they gets the same outcome but now Job 1 and Job 2 get their top picks. The key is realizing jobs can't lie to improve their own outcome *but can for others*.

5. If in a run of a jobs propose algorithm, job j is rejected by candidate c because of job j' then job j' can never be rejected by a candidate c' because of job j.

   Answer: False. Consider a three job example, where A and B proposes to 1, and C proposes to 2. B gets rejected by 1 and proposes to 2 who then rejects C. Then C proposes to 1, who rejects A who proposes to 2 who then rejects B.

4. Graphs

1. What is the least number of edges whose removal splits a 4 dimensional hypercube into two components of equal number of vertices?

   Answer: 8. It has 16 vertices, and there are 8 that connect two subcubes with 8 vertices each.

2. What is the least number of edges whose removal splits K_6 into two components of equal number of vertices?

   Answer: 9. Consider splitting the graph into two groups of size 3, the edges between the groups form $K_{3,3}$ with these vertices. That has 9 edges, three incident to each of 3 vertices on one side.

3. There is an even number of odd degree vertices in any graph.

   Answer: True. The sum of degrees is $2|E|$ and thus there must be an even number of vertices with odd degree.

4. A graph for which the average degree of vertices is an odd integer must have an odd number of vertices.

   Answer: False. If the average degree is some odd integer $2k+1$, then the total degree must be $(2k+1)v = 2kv + v$ (where v is the number of vertices). We know that the sum of degrees of a graph must be even, so v must be even.

5. What is the length (in edges) of an Eulerian tour of $G = (V, E)$?

   Answer: $|E|$. It visits every edge once.

6. For a planar graph where every face is bounded by at least 4 edges, derive an upper bound on the number of edges e in terms of v, the number of vertices.

   Answer: $2v-4$. Euler's formula states $v+f = e+2$, and each face touches ≥ 4 edges and each edge touches 2 faces, so $2e \geq 4f$ and $v + e/2 \leq e+2$ which implies $e \leq 2v-4$.

7. For a planar graph with v vertices where every face is bounded by at least 4 edges, there must be a vertex of degree less than or equal to X. What is the minimum value of X where the statement is true? (You may use U, the answer for part 6, or just state the correct number.)

   Answer: 3 or $\lfloor 2U/v \rfloor$. Since sum of degrees is $2e$, and the formula from the previous part can be used to say the sum of degrees is $4v-8$ and the average degree is at most $4-8/v$, and therefore there must be a vertex of degree at most 3.

8. For a connected graph with exactly 3 disjoint cycles, what is the minimum number of components in the graph if one removes 5 edges?

   Answer: 3. One can remove an edge in each cycle, and then removing each additional edge increases the number of components by 1.

9. If a graph does not have an Eulerian tour it does not have a Hamiltonian tour.

   Answer: False. The 3 dimensional hypercube has a Hamiltonian tour and it is not Eulerian.

5. Modular Arithmetic

1. For $x, y \in \mathbb{N}$, with $x < y$, what is the smallest M, where $y \pmod{x} < M$. (Your expression should be in terms of y only.)

   It should be as tight as possible though within 1 of the correct answer is fine.

   Answer: $y/2$. If $x > y/2$, than $y \pmod{x} = y - x < y/2$, and otherwise $y \pmod{x} < x \leq y/2$. Technically $\lfloor y/2 \rfloor$ works.

2. If $gcd(a,m) = x$ and $gcd(b,m) = y$, and $gcd(x,y) = z$, what is $gcd(ab,m)$?

   Answer: xy/z. You use the fact that each is the product of primes and m contains the primes in x and y and where the common primes in z are double counted.

3. If m and n have $gcd(m,n) = 1$, and $n = m+5$, there is a unique $x \pmod{mn}$ where $x = 5 \pmod{m}$ and $y = 0 \pmod{n}$.

   Answer: True. This is CRT. The equation $y = 0 \pmod{n}$ should have been $x = 0 \pmod{n}$. We gave everyone full credit due to this.

4. If m and n have $gcd(m,n) = 1$, and $n = m+5$, find one $x \pmod{mn}$ where $x = 5 \pmod{m}$ and $y = 0 \pmod{n}$. (Expression can possibly use m and n and should be as simple as possible for full credit.)

   Answer: n or $m+5$. This x satisfies the two equations. One could try CRT explicitly, but we expected this to be by inspection from our practice with modular arithmetic concepts. The equation $y = 0 \pmod{n}$ should have been $x = 0 \pmod{n}$. We gave everyone full credit due to this for any x where $x = 5 \pmod{m}$ regardless of whether $x = 0 \pmod{n}$.

5. How many values of $a \in \{0,\ldots,9\}$ is $f(x) \equiv ax \pmod{10}$ a bijection?

   Answer: 4.They have to have $gcd(a,10) = 1$

6. Calculate the last digit of 7^{2021}.

   Answer: 7. It is $7^{4*505+1} = (7^4)^{505} * 7 = 7$

7. If $x = y^{32}$, and $z = y^1$, give an expression for y^{65} in terms of positive powers of x and z with minimum power of z.

   Answer: $x^2 z$.

   For the following two questions. Consider $m,n \in \mathbb{N}$ where $m,n > 2$. Consider the graph G on mn vertices labeled $V = \{0,\ldots,mn-1\}$, with edges $\{(i,i+m \pmod{mn})$ and $(i,i+n \pmod{mn}) : i \in V\}$.

8. Credit only awarded if both answers are correct.

   (a) If $gcd(m,n) = 1$, what is the maximum degree of a vertex in G?

   Answer: 4. Each node appears in a cycle of vertices of length m uses edges of the form $(i,i+n)$. Similarly it appears in a cycle of vertices of length n.

   (b) If $gcd(m,n) = 1$, what is the number of connected components of G?

   Answer: 1. Using the equation $an+bm = 1$, one can use a edges of the form $(i,i+n \pmod{n})$ and b edges to get to the next higher numbered vertex. This implies that the graph is connected. It is degree 2 in each cycle and the cycles cover all incident edges.

9. Credit only awarded if both answers are correct.

   (a) If $gcd(m,n) = d$, what is the maximum degree of a vertex in G?

   Answer: 4. Each node appears in a cycle of vertices of length m uses edges of the form $(i,i+n)$. Similarly it appears in a cycle of vertices of length n. It is degree 2 in each cycle and the cycles cover all incident edges.

   (b) If $gcd(m,n) = d$, what is the number of connected components of G?

   Answer: d. A node $v \equiv i \pmod{d}$, can only reach other nodes with the same modulus i. There are d such categories. For the nodes where $v = i \mod d$, one can use the equation $an+bm = d$ to use a combination a type edges of type $(i,i+n \pmod{mn})$ and b edges of type $(i,i+m \pmod{mn})$ to change the value of v by an additive d. Thus there is a path between any pair of vertices that has the same modulus $\pmod{d}$.

6. RSA

1. For the RSA scheme where $p = 3$ and $q = 11$, choose an appropriate e and d to complete the construction.

   Answer: $e = 3, d = 7$. $7 = 3^{-1} \pmod{20}$.

2. For the RSA scheme with p and q, we have that for an integer x.
   Which of the following statements are always true? If none, state none.
   (a) $p|(x^e - x)$
   (b) $p|(x^{ed} - x)$
   (c) $p|x^{ed}$
   (d) $p|x^e$

   Answer: (b). If $x = 0$, this is true. Otherwise $x^{ed} = x^{k(p-1)(q-1)+1} = (x^{p-1})^{k(q-l)}x \equiv x \pmod{p}$. The last inequality uses Fermat's theorem.

3. Given x, y, and an RSA encryption scheme with public key where $N = pq$, what is the encryption of $E(xy)$ in terms of $E(x)$ and $E(y)$?
   Answer: $E(x)E(y) \pmod{N}$.

4. To check a signature y of a message m (that is, $y = m^d \pmod{N}$), for an RSA public key (N, e), how do you recover m? (Answer is expression involving y, N, e.)
   Answer: Compute $y^e \pmod{N}$.

7. Modular Arithmetic: Something new.

Define the order of a modulo p to be the smallest positive integer n such that $a^n \equiv 1 \pmod{p}$. Assume p is prime for this problem.

1. Compute the order of 2 modulo 7.
   Answer: 3. Note that $2^1 \equiv 2 \pmod{7}$, $2^2 \equiv 4 \pmod{7}$, and $2^3 \equiv 1 \pmod{7}$, so the order of 2 modulo 7 is 3.

2. Let d be the order of a modulo p, and suppose that $a^n \equiv 1 \pmod{p}$. Compute the value of $n \pmod{d}$. (State a value between 0 and $d-1$.)
   Answer: 0. Suppose for the sake of contradiction that $d \nmid n$. Then we can write $n = qd + r$ for integers q and r, where r is the remainder, so $0 < r < d$. Note then that we can express

   $$1 \equiv a^n \equiv a^{qd+r} \equiv a^r(a^d)^q \equiv a^r \cdot 1^q \equiv a^r \pmod{p},$$

   so we have found a positive integer r less than d such that $a^r \equiv 1 \pmod{p}$, contradicting the minimality of d. Thus, our initial assumption was incorrect, and $d \mid n$.

3. If d is the order of a modulo p, then
   (a) $d|p$
   (b) $d|(p-1)$
   Answer: (b). $d|n$ for any n where $a^n \equiv 1 \pmod{p}$ and $a^{p-1} = 1 \pmod{p}$ by FLT.

4. At most how many integers in the range $\{0, 1, 2, \ldots, p-1\}$ have order 3 modulo p? (Hint: Consider the polynomial $X^3 - 1$. Note that $X = 1$ is a solution but 1 has order 1 modulo p.)
   Answer: 2. The roots of the polynomial $X^3 - 1$ are the values a such that $a^3 \equiv 1 \pmod{p}$. From part b, the order of a modulo p divides 3. Thus, the order of a modulo p is 1 or 3. Thus, the roots of the polynomial $X^3 - 1$ are the values a such that have order 1 or 3. Thus, we need to remove the values that have order 1.
   The values that have order 1 are those such that $a^1 \equiv 1 \pmod{p}$; in other words, $a = 1$, and there is one integer in the range that has order 1. Thus, all the other roots of the polynomial $X^3 - 1$ have order 3.
   Since $X^3 - 1$ is of degree 3, it has at most 3 roots modulo p. One of these roots has order 1, so thus, there are at most 2 values modulo p that have order 3 modulo p.

8. Polynomials.

All the polynomials are over a field $GF(p)$ for a prime $p > d$ where d is the degree of the polynomial unless otherwise specified.

1. Given three points $P(1) = 1$, $P(2) = 0$, $P(3) = 0$, what is the polynomial $P(x)$ modulo 5. (Hint: this is a $\Delta_1(x)$ in Lagrange interpolation.)
   Answer: $3x^2+3$. $(x-2)(x-3)(1-2)^{-1}(1-3)^{-1} = (x^2+1)(-1)(2) = 3x^2+3$
2. If $P(x)$ is a polynomial modulo 5 of degree (at most) 1, and $P(0) = 1$ and $P(1) = 2$, what is $P(x)$?
   Answer: $x+1$. inspection.
3. Factor $x^3+4 \pmod 5$ as completely as possible. (Hint: what's the relationship between roots and factors?)
   Answer: $(x-1)(x^2+x+1)$. The idea here is to notice that the only root is 1. Thus one only needs to divide by $x-1$. To be sure, the previous problem is supposed to be helpful.
4. Every polynomial of degree exactly 1 has exactly 1 root.
   Answer: True. A degree 1 polynomial has form a_1x+a_0 and a root is at $x = -a_0(a_1)^{-1}$ and since we are working over a field a_1 has an inverse.
5. If a polynomial of degree exactly d has at least $d-1$ roots, it has exactly d roots.
   Answer: True. There are $d-1$ factors of the form $(x-r_1)\cdots(x-r_{d-1})$. What's left is a degree 1 polynomial which always has a root.
6. How many packets do you need to send to recover your original message if the length of your message is 5;
   (a) When the channel has a max of 3 erasure errors?
   Answer: $5+3 = 8$
   (b) When the channel has a max of 3 general errors?
   Answer: $5+2*3 = 11$
   (c) When the channel has a max of 2 erasure errors and 2 general errors?
   Answer: $5+2+2*2 = 11$
7. Given n points, what is the maximum value of d such that there is at most one degree d polynomial that passes through at least $n-k$ of the given points?
   Answer: $d = n-2k-1$. This is the idea that if a polynomial of degree $m-1$ is consistent with $m+k$ points out of $m+2k$ points it must be unique.
8. Consider a degree 1 polynomial $P(x) = p_1x+p_0$, and receiving four points $R(0), R(1), R(2), R(3)$ on $P(x)$ with possibly one error. (Recall that $Q(x) = P(x)E(x)$ for an error polynomial $E(x)$ in the Welch-Berlekamp scheme.)
   (a) If the error polynomial $E(x)$ is $x-e$ and $Q(x) = q_2x^2+q_1x+q_0$, what is q_1 in terms of p_0, p_1 and e?
   Answer: $-ep_1+p_0$. Just multiply out $(x-e)(p_1x+p_0)$.
   (b) Working modulo 5, given that $E(x) = x-1$ and $Q(x) = 2x^2-x-1$, what is $P(x)$?
   Answer: $2x+1$. Long division. Checking $(x-1)(2x+1) = 2x^2-x-1$.

9. Counting

1. How many anagrams of the word "SUSPICIOUS" are there?

Answer: $\frac{10!}{2!3!2!}$. We compute the number of anagrams of the word "SUSPICIOUS". There are 10! ways to order all 10 letters, and we need to divide by 3! to account for the 3 S's, 2! for the 2 I's, and 2! for the 2 U's. Thus, there are $\frac{10!}{2!3!2!}$ anagrams.

2. How many anagrams of the word "SUSPICIOUS" are there such that the letter P comes before the letter C, and the letter C comes before the letter O? For example, "PSUSICIOUS" is a valid anagram, but "SISPUCIOUS" is not.

   Answer: $\frac{10!}{2!3!2!3!}$.

   First the number of anagrams from the previous problem is $\frac{10!}{2!3!2!}$.

   Now, among the 3! possible orderings of P, C, and O among themselves, only 1 has P come before C and C come before O. Thus, we divide by 3! to get that there are $\frac{10!}{2!3!2!3!}$ valid anagrams.

   Note: the example "SISPUCIOUS" does actually meet the conditions that P, C, and O come in order, but the problem statement is fine. We graded according to the problem statement.

3. How many *strictly* increasing sequences of n integers from 1 to n are there?

   Answer: 1. Only $1,2,3,\dots,n$.

4. How many strictly increasing sequences of $n-1$ numbers chosen from 1 to n are there?

   Answer: n. One chooses a number to remove from the single increasing sequence.

5. How many sequences of n numbers from 1 to n are there where removing one number gives a strictly increasing sequence?

   Answer: $(n-1)^2+1$. Start with the numbers in order from 1 to n. If we remove any one of the n numbers and place it in one of the n positions in the arrangement, the resulting permutation will satisfy our condition, meaning we have n^2 permutations. However, there are two cases of overcounting we need to account for. The case where we end up with the original starting sequence, and the case where we have just swapped two adjacent numbers swapped. An example of the first case is if $n=3$ and decide to place 1 in the first position versus placing 2 in the second position; this results in 123. An example of the second case is if we decide to place 1 in the second position versus we decide to place 2 in the first position; either way this results in 213. Hence, we get $n^2-(n-1)-(n-1)=(n-1)^2+1$ as our final answer.

6. GME's stock price is currently \$5000 and angry Melvin Capital investors want to drive the price down. However, due to market restrictions, Melvin Capital's ability to influence GME stock price at any time is limited two possible techniques:

   - technique A: halving the price.
     For example technique A on the price \$1000 drives the price to \$500.
   - technique B: multiplying the price by $1/5$
     For example technique B on the price \$1000 drives the price to \$200.

   (a) How many different sequences of techniques are there for Melvin Capital to drive the price down to *exactly* \$5?

   Answer: Driving the price down from \$5000 to exactly \$5 involves doing technique A 3 times and technique B 3 times. There are $\binom{6}{3}$ orders in which this can be performed.

   (b) New technology enables Melvin Capital to perform one additional type of technique:

   - technique C: multiplying the price by $1/4$

   With this additional technique, how many different sequences of techniques are there for Melvin Capital to drive the price down to *exactly* \$5?

   Answer: $\binom{6}{3}+\frac{5!}{3!}$. Technique B must still be done 3 times to divide away the factors of 5. Dividing away factors of 2 can be done either with technique A 3 times (as before), or each of techniques A and C once. So we have $\binom{6}{3}+\frac{5!}{3!}$.

7. The Count is back and he has to choose a new 7-digit phone number. Again, we wants it to have the property that the digits are non-increasing. How many phone numbers are there?

   Answer: $\binom{16}{7}$. We choose 9 numbers that add up to seven and then use the numbers to indicate how many of each digit we use.

8. Consider connected graphs with n labeled vertices such that the degree of each vertex is less than 4. How many such graphs have an Eulerian tour?

   Answer: $(n-1)!/2$. To have an Eulerian tour, a graph G must be both connected and have each vertex be of even degree. The only even numbers less than 4 are 0 and 2. But a connected graph has no degree 0 vertices, so every vertex is degree 2. Then G is simply one big cycle. We only need to decide the order of connections – this is a permutation of all the labels while accounting for rotational symmetry: $\frac{n!}{n} = (n-1)!$. Further one needs to account for a symmetry as to the direction of the necklance, so we divide by 2.

10. Countability

1. Infinite ternary strings.

   Answer: Uncountable. Can diagonalize by assuming a listing and defining an string that is different in the ith position from the ith element in the listing. The object is a ternary string that is not on the list, and therefore a listing of all ternary strings does not exist.

2. The set of irrational numbers in $(0,1)$.

   Answer: Uncountable. reals in $(0,1)$ are uncountable and rational numbers in $(0,1)$ are countable. So irrational must be uncountable since the union of two countable sets is countable.

3. Constant functions $f : \mathbb{N} \to \mathbb{N}$, where $f(x) = c$ for $c \in \mathbb{N}$

   Answer: Countable. Mapping to $\mathbb{N}$ as each function corresponds to a single unique natural number.

4. A countable union of countable sets.

   Answer: Countable. Enumerate as follows. For k starting from 0 and going to infinity, for each positive i, j where $i + j = k$, output the jth element of the ith set.

5. All finite subsets of $\mathbb{N}$.

   Answer: Countable. Enumerate as follows. For k starting at 0, for all positive $i < j$ where $i + j = k$, enumerate all subsets of i sized subsets of $[1, \ldots, j]$.

11. Proof: Induction.

Show that for all positive integers n, $3^{2^n} - 1$ is divisible by 2^{n+2}. (It might be useful to recall: $(a^2 - b^2) = (a-b)(a+b)$.)

Answer: We prove the statement by induction.

Base Case: $3^{2^1} - 1$ is divisible by 8.

Inductive Step: Suppose that $3^{2^n} - 1$ is divisible by 2^{n+2} for $n = k$. We show that $3^{2^{k+1}} - 1$ is divisible by 2^{k+3}.

Note that

$$3^{2^{k+1}} - 1 = \left(3^{2^k}\right)^2 - 1 = (3^{2^k} - 1)(3^{2^k} + 1).$$

By the inductive hypothesis, the left term in the product is divisible by 2^{k+2}. Moreover, the right term in the product is divisible by 2, since it is even. Thus, $3^{2^{k+1}} - 1$ is divisible by 2^{k+3}, as desired.

The induction is complete, so we are done.

12. Proof: Graphs.

Show that a connected graph of maximum degree $d \geq 2$ can be vertex colored with d colors as long as there is at least one vertex, v, whose degree $< d$.

Answer: We use induction on the number of vertices. Remove v (whose degree $< d$) and its incident edges. Assume the remaining graph has $k \geq 1$ connected components. Each component has a vertex that is adjacent to v since the graph was initially connected. Thus, each component has a vertex with degree strictly less than d. Thus, we can color each connected component by induction. Since v has at most $d-1$ neighbors one of the d colors is available to color v.

Notice the smallest connected degree 2 graph has 3 vertices as one vertex has to have degree 2. And in fact, that graph must be a path of length 3 vertices which can be colored with 2 colors. (The triangle does not meet the condition of the claim as all vertices have the same maximum degree.)

13. Modular Arithmetic.

For this problem, let $p \equiv 3 \pmod 4$ and p is prime.

1. Show that $(p-1)/2$ is odd.

   Answer: $p = 4k+3$. $(p-1) = (4k+2) = 2k+1$ and is therefore odd.

2. Show there is no integer a such that $a^2 \equiv -1 \pmod p$. (Hint: Use Fermat's Little Theorem and the previous part.)

   Answer: Suppose for the sake of a contradiction that there exists a solution a. First, note that $a \equiv 0 \pmod p$ is not a solution. Now, suppose $a \not\equiv 0 \pmod p$. Raise both sides to the $\frac{p-1}{2}$ power. Since $p \equiv 3 \pmod 4$, $\frac{p-1}{2}$ is an odd integer. Thus, we have that

   $$1 \equiv a^{p-1} \equiv (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \pmod p,$$

   since -1 to an odd integer is -1. Thus, we have that $p \mid 1-(-1) = 2$, which is not possible, since $p \equiv 3 \pmod 4$. Thus, there is no solution to $a^2 \equiv -1 \pmod p$, as desired.

14. Combinatorial Proof.

Prove the following combinatorial identity for $n \geq 2k$.

$$k(n-2k+1)\binom{n}{k}\binom{n-k}{k-1} = 2k(2k-1)\binom{n}{2k}\binom{2k-2}{k-1}$$

(Hint: Here's a story. Count the number of ways to create two groups of size k out of n people where exactly one person to be in both groups, and designate one person not in a group as the leader.)

Answer: LHS: We first pick the k people to be in group 1. We select one person who will also be in group 2. Then, we choose $k-1$ other people to be in group 2 from the $n-k$ people not in group 1. Lastly, we choose our leader from the $(n-2k+1)$ unchosen people.

RHS: Here, we initially select $2k$ people to be in our setup. Pick one of them to be the captain $(2k)$, then pick another to be in both groups $(2k-1)$. Lastly, of the $(2k-2)$ people that go into exactly one group, choose $k-1$ of them to be in group 1 (and the rest go in group 2).