Problem Set 4

Due: Monday, October 3

Reading Assignment: Sections 4.5.1, 4.6.4, 4.8, 5.0, 5.1, 5.3

Problem 1. [15 points] Euler's theorem states that for any integer n, if a is **relatively prime** to n, then $a^{\phi(n)} \equiv 1 \pmod{n}$, where $\phi(n)$ is referred to as the Euler totient function ($\phi(n)$ is also equal to the number of positive integers less than n that are relatively prime to n). In particular, if $n = pq$ for primes p, q, then $\phi(n) = (p-1)(q-1)$.

(a) [10 pts] In RSA, we used an application of Euler's theorem to essentially "conclude" that $m^{ed} \equiv m \pmod{pq}$ for integers e, d such that $ed \equiv 1 \pmod{(p-1)(q-1)}$. But what happens if $m = p$ or $m = q$? Clearly, we have that p and q are not relatively prime to pq. Nevertheless, show that if $m = p$ or $m = q$, we still have that $m^{ed} \equiv m \pmod{pq}$.

(b) [5 pts] Suppose Alice and Bob are communicating using RSA. Alice generates a pair of primes, and computes N_A, which is the product of those primes. Similarly, Bob generates a pair of primes, and computes N_B, which is the product of those primes. Unfortunately, one of the primes Bob uses to construct N_B is the same as one of those Alice used to construct N_A. How can a third party Eve now eavesdrop on communications between Alice and Bob if $N_A \neq N_B$?

Problem 2. [15 points] In this problem, we will investigate systems of linear congruence equations.

(a) [5 pts] Find the smallest positive integer x, which leaves a remainder 1 when divided by 3 and leaves a remainder 3 when divided by 7. (*Hint*: If x leaves a remainder 1 when divided by 3, write $x = 1 + 3k_1$ for some integer k_1, and consider $1 + 3k_1 \equiv 3 \pmod{7}$)

(b) [10 pts] For integers a and b and for relatively prime integers m, n, find a range of solutions to

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

Problem 3. [15 points] Recall that a ***coloring*** of a simple graph is an assignment of a color to each vertex such that no two adjacent vertices have the same color. A ***k-coloring*** is a coloring that uses at most k colors.

False Claim. *Let G be a (simple) graph with maximum degree at most k. If G also has a vertex of degree less than k, then G is k-colorable.*

(a) [5 pts] Give a counterexample to the False Claim when $k = 2$.

(b) [10 pts] Consider the following proof of the False Claim:

Proof. Proof by induction on the number n of vertices:

Induction hypothesis: $P(n)$ is defined to be: Let G be a graph with n vertices and maximum degree at most k. If G also has a vertex of degree less than k, then G is k-colorable.

Base case: (n=1) G has only one vertex and so is 1-colorable. So $P(1)$ holds.

Inductive step:

We may assume $P(n)$. To prove $P(n+1)$, let G_{n+1} be a graph with $n+1$ vertices and maximum degree at most k. Also, suppose G_{n+1} has a vertex, v, of degree less than k. We need only prove that G_{n+1} is k-colorable.

To do this, first remove the vertex v to produce a graph, G_n, with n vertices. Removing v reduces the degree of all vertices adjacent to v by 1. So in G_n, each of these vertices has degree less than k. Also the maximum degree of G_n remains at most k. So G_n satisfies the conditions of the induction hypothesis $P(n)$. We conclude that G_n is k-colorable.

Now a k-coloring of G_n gives a coloring of all the vertices of G_{n+1}, except for v. Since v has degree less than k, there will be fewer than k colors assigned to the nodes adjacent to v. So among the k possible colors, there will be a color not used to color these adjacent nodes, and this color can be assigned to v to form a k-coloring of G_{n+1}. □

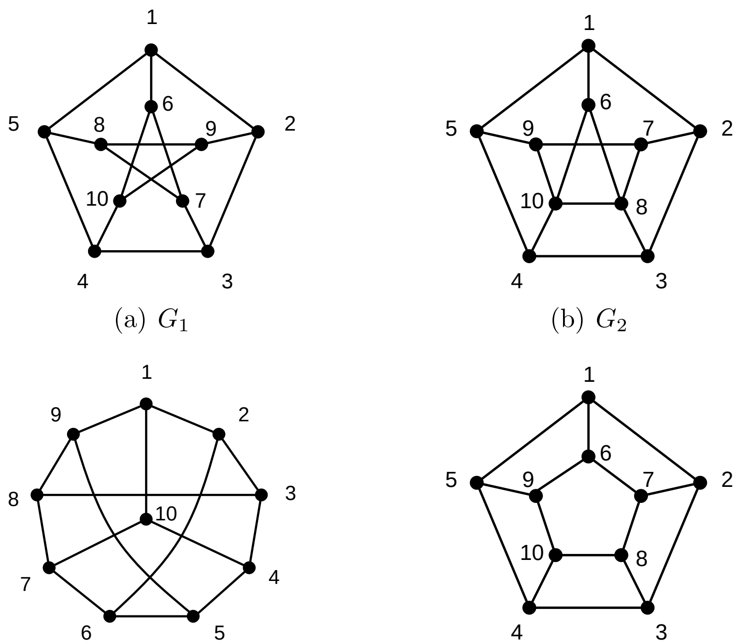
Identify the exact sentence where the proof goes wrong.

Problem 4. [15 points] Two graphs are isomorphic if they are the same up to a relabeling of their vertices (see Definition 5.1.3 in the book). A property of a graph is said to be *preserved under isomorphism* if whenever G has that property, every graph isomorphic to G also has that property. For example, the property of having five vertices is preserved under isomorphism: if G has five vertices then every graph isomorphic to G also has five vertices.

(a) [5 pts] Some properties of a simple graph, G, are described below. Which of these properties is *preserved under isomorphism*?

1. G has an odd number of vertices.
2. None of the labels of the vertices of G is an even integer.
3. G has a vertex of degree 3.
4. G has a exactly one vertex of degree 3.

(b) [10 pts] Determine which among the four graphs pictured in the Figures are isomorphic. If two of these graphs are isomorphic, describe an isomorphism between them. If they are not, give a property that is preserved under isomorphism such that one graph has the property, but the other does not. For at least one of the properties you choose, *prove* that it is indeed preserved under isomorphism (you only need prove one of them).



(a) G_1 (b) G_2

(c) G_3 (d) G_4

Figure 1: Which graphs are isomorphic?

Problem 5. [20 points] 6.042 is often taught using recitations. Suppose it happened that 8 recitations were needed, with two or three staff members running each recitation. The assignment of staff to recitation sections is as follows:

- R1: Henry, Emanuele, Rachel
- R2: Henry, Wei-En, Sean
- R3: Emanuele, Devin
- R4: Tally, Wei-En, Michael
- R5: Tally, Patrick, Sean
- R6: Patrick, Devin
- R7: Patrick, Wei-En

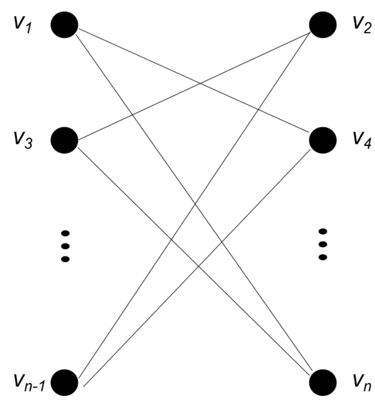
- R8: Emanuele, Devin, Sean

Two recitations can not be held in the same 90-minute time slot if some staff member is assigned to both recitations. The problem is to determine the minimum number of time slots required to complete all the recitations.

(a) [10 pts] Recast this problem as a question about coloring the vertices of a particular graph. Draw the graph and explain what the vertices, edges, and colors represent.

(b) [10 pts] Show a coloring of this graph using the fewest possible colors. What schedule of recitations does this imply?

Problem 6. [20 points] Suppose you have a graph as shown below. Every node on the left is adjacent to every node on the right except the node directly across from it.



(a) [5 pts] Find the chromatic number of the graph.

(b) [5 pts] The graph pictured above is often referred to as *bipartite*.

Definition. *A graph $G = (V, E)$ is bipartite if the set of vertices, V, can be split into two subsets V_l and V_r such that all edges in G connect nodes in V_l to nodes in V_r.*

Now recall from lecture the Greedy Coloring Algorithm:
Greedy Coloring Algorithm: For a graph $G = (V, E)$ and an ordering of vertices $v_1, v_2, \cdots, v_n$

1. Color v_1 with a new color c_1.
2. For each vertex v_i, if v_i shares an edge with with any earlier vertex, v_j, colored c_k, then it cannot be colored c_k. Choose the lowest available color for v_i.

Find an ordering of the vertices $\{v_1, v_2, \cdots, v_n\}$ such that the Greedy Coloring Algorithm uses exactly 2 colors.

(c) [5 pts] Find an ordering such that the Greedy Coloring Algorithm uses exactly $n/2$ colors.

(d) [5 pts] Prove your answer in part (c) by induction for all even integers n.