6.042/18.062J Mathematics for Computer Science September 27, 2016
Tom Leighton and Ankur Moitra

Problem Set 4 Solutions

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 $m^{ed} \equiv m \pmod{pq}$.

Rubric
[10pts] Any correct proof.

or

[5pts] $p^{1+k(p-1)(q-1)} \equiv p \pmod{pq}$ or $pq \mid p^{1+k(p-1)(q-1)} - p$ ($1 + k(p-1)(q-1)$ can be replaced by ed
[5pts] $q \mid p^{k(p-1)(q-1)} - 1$ by Fermat's little theorem.

Solution. We will show that the statement holds for $m = p$. Then by symmetry, we can conclude that the statement holds for $m = q$. First, if $ed \equiv 1 \pmod{(p-1)(q-1)}$, then there exists some integer k such that $ed = 1 + k(p-1)(q-1)$ by definition. Hence we must show that $p^{1+k(p-1)(q-1)} \equiv p \pmod{pq}$. But this is equivalent to showing that $pq \mid p^{1+k(p-1)(q-1)} - p$.

Now $p^{1+k(p-1)(q-1)} - p = p(p^{k(p-1)(q-1)} - 1)$. Hence we just need to show that $q \mid p^{k(p-1)(q-1)} - 1$. But this is true by Fermat's little theorem as p, q are relatively prime. ■

(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 $N_A \neq N_B$?

Rubric
[2pts] gcd of (N_A, N_B) will be prime p.
[2pts] $\frac{N_A}{p}, \frac{N_B}{p}$ gives the other primes.
[1pt] Use Pulverizer to find d.

Solution. First Eve calculates the gcd of (N_A, N_B), which must be the common prime p used by both Bob and Alice since $N_A \neq N_B$ and each of N_A, N_B is a product of exactly two primes. Hence Eve can then compute $\frac{N_A}{p}, \frac{N_B}{p}$ to find the primes that Alice and Bob are using. Now, given Alice and Bob's public keys, Eve can then use the Pulverizer to compute their private keys. Hence, Eve is then able to completely unravel the RSA scheme used by Alice and Bob. ■

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 $1 + 3k_1 \equiv 3 \pmod 7$)

Rubric
[-1pt] Math errors.
[5pts] $x = 10$.

Solution. As suggested in the hint, we let $x = 1 + 3k_1$. Then we consider

$$\begin{aligned} 1 + 3k_1 &\equiv 3 \pmod 7 \\ 3k_1 &\equiv 2 \pmod 7 \\ k_1 &\equiv 10 \pmod 7 \quad \text{Since we have that the inverse of 3 mod 7 is 5} \end{aligned}$$

Now by definition, there must be some integer k_2 for which $k_1 = 10 + 7k_2$. Substituting back into the equation for x, we conclude that $x = 1 + 3(10 + 7k_2) = 31 + 21k_2$. Hence we substitute $k_2 = -1$ to find the smallest positive integer $x = 10$. ■

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

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

Rubric
[-1pt] Math errors.
[6pts] Follow the same steps as taken in part (a).
[4pts] $x = a + (s(b - a) + nk_2)m$ or $a + s(b - a)m + nmk_2$.

Solution. We follow the same procedure outlined in the part above. Since $x \equiv a \pmod{m}$, let $x = a + k_1 m$ for some integer k_1. Then substitute this equation into $x \equiv b \pmod{n}$:

$$\begin{aligned} a + mk_1 &\equiv b \pmod{n} \\ mk_1 &\equiv b - a \pmod{n} \\ k_1 &\equiv s(b-a) \pmod{n} \text{ Where s is the inverse of m mod n} \end{aligned}$$

Now by definition, there must be some integer k_2 for which $k_1 = s(b-a)+nk_2$. Substituting back into the equation for x, we conclude that:

$x = a + (s(b-a) + nk_2)m = a + s(b-a)m + nmk_2$

is a range of solutions to the system of congruences.

■

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 $k = 2$.

Rubric
[5pts] Any correct counterexample

or

[5pts] One node by itself, and a separate triangle.

Solution. One node by itself, and a separate triangle (K_3). The graph has max degree 2, and a node of degree zero, but is not 2-colorable. ■

(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.

Rubric
[10pts] Correct sentence with correct reasoning.

or

[5pts] Correct reasoning of "if v has degree 0, then removing v will not reduce the degree of any vertex, and so there may not be any vertex of degree less than k in G_n"

and one of

[3pts] Removing v reduces the degree of all vertices adjacent to v by 1.
[5pts] So in G_n, each of these vertices has degree less than k.

Solution. "So G_n satisfies the conditions of the induction hypothesis $P(n)$." The flaw is that if v has degree 0, then removing v will not reduce the degree of any vertex, and so there may not be any vertex of degree less than k in G_n, as in the counterexample of part (a)." ■

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.

Rubric
[-1pt] For each wrong answer. 1, 3, and 4 are preserved

Solution. 1. It is invariant under isomorphism. There must be an one-to-one and onto mapping between the vertices of two isomorphic graphs. Therefore, the number of vertices in the two graphs must be the same. If one graph has odd number of vertices, then the other must have odd number of vertices.

2. It is not invariant under isomorphism. We do not really care what the labels of vertices are. Vertices can be any kind of mathematical objects. All we are interested is that whether there exists a one-to-one and onto function f mapping from vertices of one graph to vertices of another with the property that a and b are adjacent in the first graph if and only if $f(a)$ and $f(b)$ are adjacent in the second graph, for all a and b in the first graph.

   So, for example, let G_1 be a graph with a single vertex, 1, and G_2 be a graph with a single vertex, 2. Obviously the two graphs are isomorphic, but G_1 does not have vertices which are even integers.

3. It is invariant under isomorphism.

   Let G_1, G_2 be simple graphs and $f : V_1 \to V_2$ be an isomorphism between them. Suppose $v \in V_1$ has degree 3; we want to show that there is a vertex of degree 3 in V_2. In fact, we'll show that $f(v)$ has degree 3.

   Since v has degree 3, there are exactly 3 vertices adjacent to v; say these are v_1, v_2, v_3. Since f is a bijection, $f(v_1), f(v_2)$ and $f(v_3)$ are all distinct. Since there is an edge between v and v_i in G_1, the definition of isomrphism implies that there is an edge between $f(v)$ and $f(v_i)$ for $i = 1, 2, 3$, so the degree of $f(v)$ is at least 3.

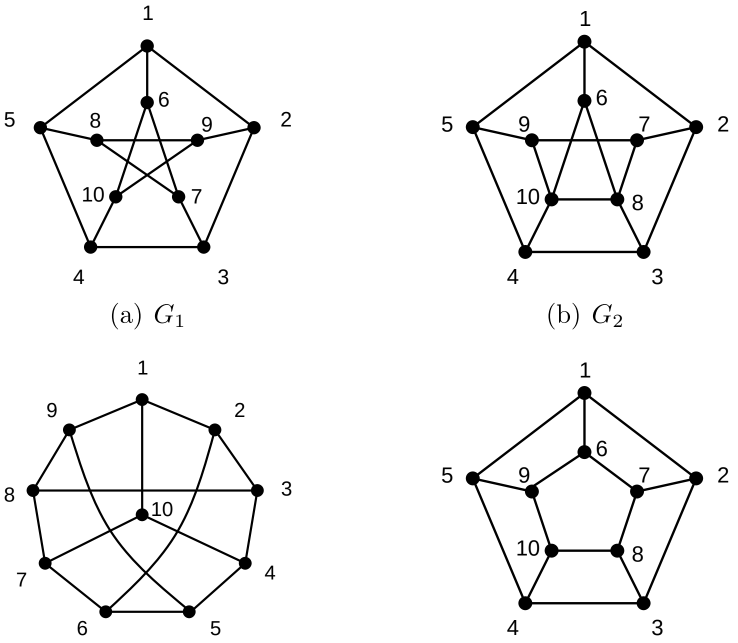
   We now prove by contradiction that the degree of $f(v)$ is at most 3. Suppose $f(v)$ had degree > 3. This means there is a vertex $w \in V_2$ which is not equal to $f(v_1), f(v_2)$, or $f(v_3)$, but is also adjacent to $f(v)$. Since, f is a bijection, there is a vertex $v_4 \in V_1$ such that $f(v_4) = w$ and $v_4 \neq v_i$ for $i = 1, 2, 3$. Since $w = f(v_4)$ is adjacent to $f(v)$, the definition of isomorphism implies that v_4 is adjacent to v, contradicting the fact the v_1, v_2, v_3 were exactly the vertices adjacent to v.

4. It is invariant under isomorphism.

   Prove by contradiction: Suppose a graph G_1 has exactly one vertex of degree 3 while another graph G_2 does not have exactly one vertex of degree 3. Suppose the two graphs are isomorphic. If G_2 does not have a vertex of degree 3, then from part (c), there is a contradiction. If G_2 has more than one vertex of degree 3, then there must be at least one vertex in G_2 of degree 3 which is mapped to a vertex of degree $\neq 3$ in G_1. Since two vertices of different degrees are mapped from G_1 to G_2, using the same argument from part (c), it reaches a contradiction. Therefore, if G_1 has exactly one vertex of degree 3, then G_2 must also have 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?

Rubric
[1pt] G_1 and G_3 are isomorphic.
[2pts] Correct isomorphism.
[1pt] G_2 is not isomorphic to G_1 or G_4.
[1pt] Correct justification for why G_2 is not isomorphic to G_1 or G_4.
[1pt] G_4 is not isomorphic to G_1 or G_2.
[1pt] Correct justification for why G_4 is not isomorphic to G_1 or G_2.
[3pts] Proof for one of the property on why it is preserved under isomorphism. (See (a)).

Solution. G_1 and G_3 are isomorphic. In particular, the function $f : V_1 \to V_3$ is an isomomorphism, where

$$\begin{array}{lllll} f(1) = 1 & f(2) = 2 & f(3) = 3 & f(4) = 8 & f(5) = 9 \\ f(6) = 10 & f(7) = 4 & f(8) = 5 & f(9) = 6 & f(10) = 7 \end{array}$$

G_1 and G_4 are not isomorphic to G_2: G_2 has a vertex of degree four and neither G_1 nor G_4 has one.

G_1 and G_4 are not isomorphic: G_4 has a simple cycle of length four and G_1 does not.

■

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:

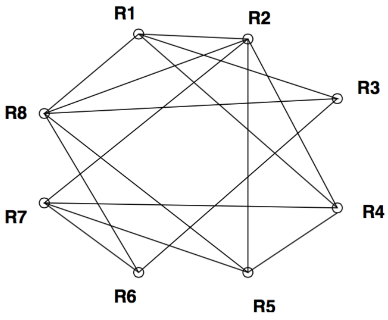
- R1: Henry, Emanuele, Rachel
- R2: Henry, Wei-En, Sean
- R3: Emanuele, Devin
- R4: Tally, Wei-En, Michael
- R5: Tally, Patrick, Sean
- R6: Patrick, Devin
- R7: Patrick, Wei-En
- R8: Emanuele, Devin, Sean

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.

Rubric
[2pts] Vertex is a recitation section.
[2pts] Edge connects recitations that cannot be scheduled at same time.
[2pts] Color corresponds to time slot.
[3pts] Correctly drawn graph.

Solution. Each vertex in the graph below represents a recitation section. An edge connects two vertices if the corresponding recitation sections share a staff member and thus can not be scheduled at the same time. The color of a vertex indicates the time slot of the corresponding recitation.

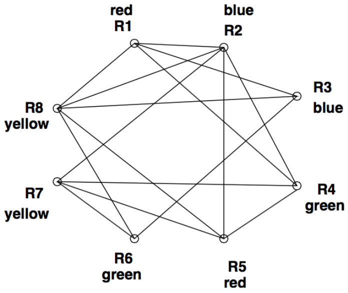


■

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

Rubric
[7pts] Any valid grouping of recitations. (Should be right if the number of time slots is)
[3pts] 4 time slots because 4 colors.

Solution. Four colors are necessary and sufficient. To see why they are *sufficient*, consider the coloring:



This corresponds to the following assignment of recitations to four time slots:

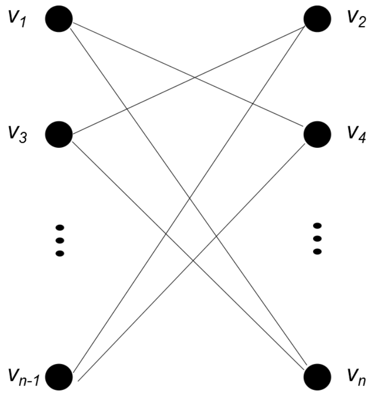
1. R1, R5

2. R2, R3
3. R4, R6
4. R7, R8

Other schedules are also possible.

To see why 4 colors are *necessary*, look at the subgraph defined by the vertices for R2, R4, R5, and R7. This is the complete graph on 4 vertices, and it obviously needs 4 colors. ■

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.

Rubric
[5pts] 2 colors.

Solution. We can color each node on the left side with red and each node on the right with blue since no edges form between nodes on the same side. Thus, the chromatic number is 2. ■

(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.

Rubric
[5pts] $v_1, v_3, v_5, \cdots v_{n-1}, \cdots, v_2, v_4, \cdots, v_n$

Solution. Since none of the vertices on the left share an edge, we can color all of them with the same color, so we iterate through all the left nodes, then all the right nodes with the ordering, $v_1, v_3, v_5, \cdots v_{n-1}, \cdots, v_2, v_4, \cdots, v_n$. The left side uses only one color and the right side uses only one color similar to the solution in part (a). ■

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

Rubric
[5pts] Alternating sides

Solution. Notice that alternating across left and right with the greedy algorithm forces us to pick a new color every time we are on the left side. Thus, we can choose the ordering $v_1, v_2, \cdots v_{n/2}, \cdots v_n$ to get $n/2$ colors. ■

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

Rubric
[0pts] Not a proof by induction

or

[1pt] Induction hypothesis
[1pt] Base case
[1pt] Show $P(n)$ implies $P(n+2)$
[2pts] Corrective inductive step

Solution. *Proof.* $P(n)$ is defined to be: For a bipartite graph with n vertices (labeled in the pattern as shown in the graph), with edges as shown in the graph, applying the Greedy Coloring Algorithm to the vertex ordering $v_1, v_2 \cdots v_n$ uses exactly $n/2$ colors for all even integers n. In addition, the coloring consists of the first $n/2$ colors on each side across from one another.

Base Case (n = 2) There are no edges in this case, so the Greedy Coloring Algorithm uses only one color.

Inductive Step Assume that $P(n)$ is true. We will show that this implies $P(n+2)$. Denote our two new nodes v_{n+1} and v_{n+2}. v_{n+1} is connected to $\{v_2, v_4, \cdots v_n\}$ and v_{n+2} is connected to $\{v_1, v_3, \cdots v_{n-1}\}$. Since by $P(n)$, v_{n+1} is connected to $n/2$ different colors, the Greedy Coloring Algorithm will choose a different color $c_{n/2+1}$. For v_{n+2}, the Greedy Algorithm will color it $c_{n/2+1}$ since its connected to $v_1, v_3, \cdots v_{n-1}$ which are the first $n/2$ colors. Thus, the new nodes are both a new color.

Thus, by induction, $P(n+2)$ is true.

□

■