n

Math 280: Graph Theory
Instructor: David Zureick-Brown ("DZB")

All assignments
Last updated: August 26, 2024
Gradescope code: VD5BZK

Show all work for full credit!
Proofs should be written in full sentences whenever possible.

Contents

Assignment 1: Introduction to the course

Due by 12:55pm, eastern, on Thursday (tentative), Sept ??

Suggested readings for this problem set:

- Syllabus: https://dmzb.github.io/teaching/2024Fall280/syllabus-math-280-spring-2024.pdf
- Sections 1.1.1 and 1.1.2 and start 1.1.3

All readings are from Harris, Hirst, and Mossinghoff, *Combinatorics and Graph Theory*.

Assignment: due Thursday (tentative), Sept ??, 12:55pm, via Gradescope (VD5BZK):

1. If G is a graph of order n, what is the maximum possible size of G? (That is, what's the maximum possible number of edges G could have?)

   Don't forget to justify your answer! You don't need to give a formal proof on this more computational problem, but you need to explain why you know your answers are correct.

2. Let G be a graph of order $n \geq 2$. Prove that the degree sequence of G has at least one pair of repeated entries.

   (*Suggestion*: What degrees are possible in such a graph G? And use the pigeonhole principle.)

   For this graph:
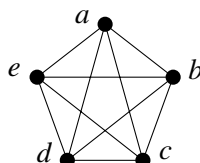
   (c) What is the maximum length of a circuit in this graph? Give an example of such a circuit.

   (d) What is the maximum length of a circuit that does not include vertex c? Give an example of such a circuit.

   Don't forget to justify your answers! You don't need to give a formal proof on this more computational problem, but you need to explain why you know your answers are correct.

3. Let G be a graph of odd order. Suppose that all the vertices of G have the same degree r. Prove that r is an even number.

   Prove that every closed walk of odd length in a graph contains a cycle of odd length.

4. Let G be a graph of order n and size t. Let $\overline{G}$ be the complement graph of G. (See the textbook, Section 1.1.3, item 3.) Find the order and size of $\overline{G}$.

   Don't forget to justify your answers!

5. Let X be the following graph:
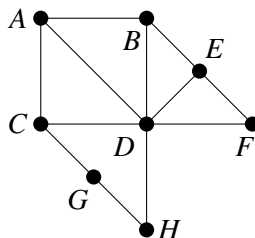
   (a) Find the degree sequence of X.

   (b) Find the longest trail in X. Justify why it is the longest.

   (c) Find the longest path in X. Justify why it is the longest.

   (d) Draw the complementary graph to G.

6. Given a graph G of order n and size d determine the order and size of its complementary graph $\overline{G}$. Justify your answer.

7. Prove that if u is a vertex of odd degree in a graph, then there exists a path from u to another vertex v of the graph where v also has odd degree.

8. There are n Amherst students participating in a meeting. Among any group of 4 participants, there is one who knows the other three members of the group. Prove that there is one participant who knows all other participants.

9. Let G be a graph with 10 vertices. Among any three vertices of G, at least two are adjacent. Find the least number of edges that G can have. Find a graph with this property.

Assignment 2: Basic properties, e.g., connectedness

Due by 12:55pm, eastern, on Thursday (tentative), Sept ??

Suggested readings for this problem set:

- Section 1.1.3 and start 1.2.1

All readings are from Harris, Hirst, and Mossinghoff, *Combinatorics and Graph Theory*.

Assignment: due Thursday (tentative), Sept ??, 12:55pm, via Gradescope (VD5BZK):

1. Let G be a 2-connected graph. Prove that G contains at least one cycle.

   (*Suggestion*: Remember that 2-connected means that if you delete any one vertex v, the subgraph $G - v$ is still connected, which means for any two of the remaining vertices, there's a path between them that avoids v.)

2. (a) Let G be a graph of order n such that $\delta(G) \geq (n-1)/2$. Prove that G is connected.

   (b) For any positive even integer $n = 2m \geq 2$, find a graph G of order n such that $\delta(G) \geq (n-2)/2$ but G is *not* connected.

   (*Suggestion*: For both (a) and (b), think about what the two separate components of G would have to look like.)

3. Is K_4 a subgraph of $K_{4,4}$? (More precisely, is there a subgraph of $K_{4,4}$ isomorphic to K_4, i.e., that is a complete graph on 4 vertices?) If yes, exhibit one explicitly. If no, prove no such subgraph exists.

4. Let G and H be isomorphic graphs. Prove that their complements $\overline{G}$ and $\overline{H}$ are also isomorphic.

5. Consider the following two graphs:
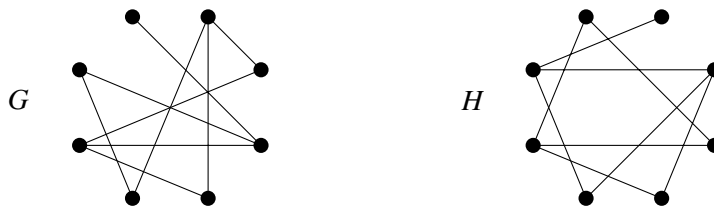
   Verify that G and H have the same order, same size, and same degree sequence.

   Then prove that in spite of that, G and H are *not* isomorphic.

6. Let G be a simple graph. Prove that the degree sequence of G has at least one repeated element.

7. Prove that if x belongs to the periphery of a graph G and $d(x,y) = ecc(x)$, then y belongs to the periphery of G.

8. Show that if every connected component of a graph is bipartite, then the graph is bipartite.

9. Suppose G is a simple graph that has ten edges, and six vertices $v_1, v_2, \ldots v_6$ with degrees $2, 2, 3, 4, 4, n$, respectively, for some integer n.

    (a) What is the integer n, i.e., $\deg(v_6)$?

    (b) Is G connected? (Yes, no, or maybe?) If "maybe," give an example of such a graph G that is connected, and another that is not connected.


Assignment 3: Walks

Suggested readings for this problem set:

- Section 1.2.1–1.2.3

All readings are from Harris, Hirst, and Mossinghoff, *Combinatorics and Graph Theory*.

Assignment: due Thursday (tentative), Sept ??, 12:55pm, via Gradescope (VD5BZK):

---

1. Suppose G is a graph that has 10 edges and 6 vertices, and suppose that the degrees of five of those vertices are $2, 2, 3, 4, 4$, and the sixth has some degree n.

   (a) Find the integer n, i.e., the degree of the sixth vertex.

   (b) Is G connected? (Yes, no, or maybe?) If "yes" or "no", prove it; if "maybe", draw two examples of such a graph G: one that is connected and one that is not.

2. For each of the graphs P_5, C_5, and K_5:

   (a) draw the graph

   (b) find the eccentricity of each vertex

   (c) find the radius and diameter of the graph

   (d) find its adjacency matrix.

   (For P_5, number the vertices 1 to 5 from one end to the other; for C_5, label them consecutively around the cycle.)

3. Find the radius, diameter, and center of the following graph:
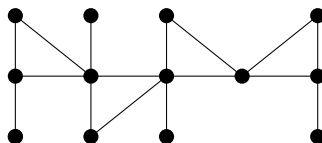
4. Let G be a graph, and let $u, v \in V(G)$ be adjacent vertices. Prove that their eccentricities $\text{ecc}(u)$ and $\text{ecc}(v)$ differ by at most 1.

5. (a) Draw a graph of order 7 that has radius 3 and diameter 6.

   (b) Draw a graph of order 7 that has radius 3 and diameter 5.

   (c) Draw a graph of order 7 that has radius 3 and diameter 4.

   In all three cases, don't forget to (briefly) justify that your graph has the correct order, radius, and diameter.

6. Let G be the following graph:
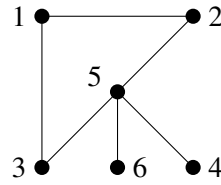
   (a) Find the adjacency matrix A of G.

   (b) Find all the walks of length 3 from vertex 1 to vertex 4. What is the total number of such walks, and (without computing A^3) what does this say about the matrix A^3?

   (c) How many closed walks of length 3 are there in G? Without computing A^3, how would this number be related to the matrix A^3?

   (d) Find the eccentricities of all the vertices of G.

   (e) Find the radius, diameter, center and periphery of G.

7. Let G be a graph with $V(G) = \{v_1, \ldots, v_n\}$ and with adjacency matrix A. For each $j = 1, \ldots, n$, prove that the (j, j) entry of A^2 is $\deg(v_j)$.

8. Let $A = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$, and let G be the graph with adjacency matrix A.

   (a) Compute A^2 and A^3.

   (b) How many walks are there in G from vertex 1 to vertex 2 of length exactly 3?

   (c) Find the radius and the diameter of G.

   (d) Draw the graph G and determine in your drawing the center and periphery of G.

Assignment 4: Trees

Due by 12:55pm, eastern, on Thursday (tentative), Sept ??

Suggested readings for this problem set:

- Sections 1.3.1–1.3.3 and start 1.3.4

All readings are from Harris, Hirst, and Mossinghoff, *Combinatorics and Graph Theory*.

Assignment: due Thursday (tentative), Sept ??, 12:55pm, via Gradescope (VD5BZK):

---

1. Draw all unlabeled trees of order 7.

   (More precisely: Find a set of trees of order 7 so that *every* tree of order 7 is isomorphic to one in your set, and so that no two in your set are isomorphic to each other.)

   (*Hint*: there are 11 of them. Careful not to draw the same one twice in a different way! You don't need to give a formal proof that your set is complete; just draw 11 truly different trees of order 7. Make sure to draw **clearly**; unclear graphs will be marked wrong.)

2. Let T be a tree of order $n \geq 2$. Prove that T is bipartite.

   (*Hint*: Do we know any theorems about when a graph is bipartite?)

3. Let T be a tree that has an even number of edges. Prove that at least one vertex of T has even degree.

4. Let T be a tree, and let $u, v \in V(T)$. Prove that there is *exactly one* path from u to v.

5. Let T be a tree, and let $u, v \in V(T)$ be two distinct vertices that are *not* adjacent. Define a new graph G with the same vertex set $V(G) = V(T)$ but with one extra edge $e = uv$. That is, $E(G) = E(T) \cup \{e\}$, where the new edge e runs between u and v.

   Prove that the new graph G has exactly one cycle.

   (*Suggestion*: Use the result of the previous problem.)

6. Let T be a tree of order $n \geq 2$, and suppose that none of the vertices of T have degree 2. Prove that T has more than $n/2$ leaves.

7. Let G be a connected graph. Prove that G contains at least one spanning tree.

   (*Suggestion*: for any subtree T that is missing at least one vertex, show that there is a larger subtree T' of G that contains all of T and one more vertex.)

Assignment 5: Spannign trees; Prüfer sequences

Due by 12:55pm, eastern, on Thursday (tentative), Sept ??
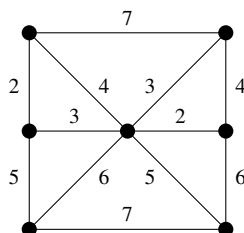
Suggested readings for this problem set:

- Sections 1.3.4 and 1.4.1

All readings are from Harris, Hirst, and Mossinghoff, *Combinatorics and Graph Theory*.

Assignment: due Thursday (tentative), Sept ??, 12:55pm, via Gradescope (VD5BZK):

1. Use Kruskal's algorithm to find a minimum weight spanning tree of the following graph. Be sure to (briefly!) show your steps.

2. Use Prüfer's method to find the Prüfer sequences of the following two trees. As always, (briefly) show your steps.
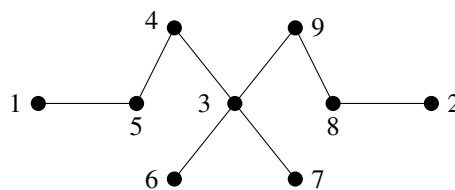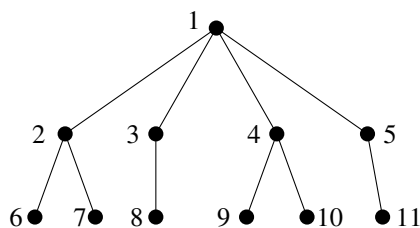
3. Use Prüfer's method to draw and label a tree with Prüfer sequence 5,4,3,5,4,3,5,4,3. As always, (briefly) show your steps.

4. Let T be a labeled tree, and let σ be its Prüfer sequence. For each vertex $v \in V(T)$, prove that v appears in σ exactly $\deg(v) - 1$ times.

   (*Suggestion*: Do an induction on $n \geq 2$, where n is the order of the tree.)

   (*Note*: As a special case, this means that none of the leaves of T appear in the sequence σ at all. The textbook states that as a separate fact, but since it's just a special case of the above statement, you only need to prove the above statement.)

5. For each of the following four graphs, write down its Laplacian matrix, and then use the Matrix Tree Theorem to find its number of spanning trees.

$$P_4 \qquad\qquad C_4 \qquad\qquad K_4 \qquad\qquad K_{2,3}$$

6. (a) Use Prüfer's method to draw and label the trees with Prüfer sequences 1,1,1,1,1 and 3,3,3,3.

   (b) Inspired by your answers in part (a), make a conjecture about which trees have constant Prüfer sequences.

   (c) Prove your conjecture from part (b).

Midterm 1 study guide

Content: The questions will all be either

1. homework problems,

2. suggested problems,

3. problems we worked in class, or

4. minor variations of one of these.

Problems with very long proofs or that involved some unusual trick will not be on the exam.

You are allowed to use any previous problem from class or from the homework (e.g., "additivity of divisibility" or "the 2 out of 3 rule") on the exam without reproving it, unless otherwise noted on the exam. (E.g., if I ask you to prove "additivity of divisibility" on the exam, you will need to prove this using only the definition of divisibility, and I will remind you of this in the statement of the problem.)

A typical exam will have one or two questions from each week of the course and will cover **assignments 1-5**. You can expect problems about following:

- TBA.

Assignment 6: Matrix Tree Theorem; Eulerian and Hamiltonian graphs

*Due by 12:55pm, eastern, on Thursday (tentative), Sept ??*

Suggested readings for this problem set:

- Sections 1.3.4 and 1.4.2 , and start 1.4.3

All readings are from Harris, Hirst, and Mossinghoff, *Combinatorics and Graph Theory*.

Assignment: due Thursday (tentative), Sept ??, 12:55pm, via Gradescope (VD5BZK):

1. (a) Use Prüfer's method to draw and label the trees with Prüfer sequences 1,2,3 and 3,4,1,2.

   (b) Inspired by your answers in part (a), make a conjecture about which trees have Prüfer sequences consisting of all distinct terms.

   (c) Prove your conjecture from part (b).

2. Use the Matrix Tree Theorem to find the number of spanning trees of this graph:
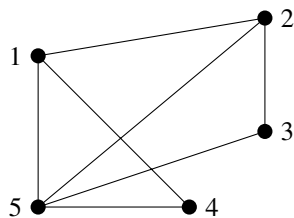
3. Let G be a graph with Laplacian matrix Δ. Prove that $\det(\Delta) = 0$.

   (**Suggestion**: Remember that invertible matrices have trivial nullspace, and that nonzero determinant implies the matrix is invertible.)

4. Determine the values of $m, n \geq 1$ such that the complete bipartite graph $K_{m,n}$ is Eulerian. Prove your answer.

5. Determine the precise set of values of $m, n \geq 1$ such that the complete bipartite graph $K_{m,n}$ has an Eulerian trail. Prove your answer.

6. For each of the following, draw an Eulerian graph the satisfies the conditions, or prove that no such graph exists.

   (a) An even number of vertices, and an even number of edges.

   (b) An even number of vertices, and an odd number of edges.

   (c) An odd number of vertices, and an even number of edges.

   (d) An odd number of vertices, and an odd number of edges.

7. For the graph $G = K_5$, determine:

    (a) is it Eulerian?   (b) is it Hamiltonian?

    (c) is it traceable?   (d) what is its independence number $\alpha(G)$?

As always, be sure to (briefly) justify your answers.

8. For the graph $G = P_7$, determine:

    (a) is it Eulerian?   (b) is it Hamiltonian?

    (c) is it traceable?   (d) what is its independence number $\alpha(G)$?

As always, be sure to (briefly) justify your answers.

Assignment 7: Independence; Planar graphs

Due by 12:55pm, eastern, on Thursday (tentative), Sept ??

Suggested readings for this problem set:

- <mark>Sections 1.4.3 and 1.5.1</mark> ,
- lightly read 1.4.4, and start 1.5.2

All readings are from Harris, Hirst, and Mossinghoff, *Combinatorics and Graph Theory*.

Assignment: due Thursday (tentative), Sept ??, 12:55pm, via Gradescope (VD5BZK):

1. For the graph $G = C_4$, determine:

    (a) is it Eulerian?   (b) is it Hamiltonian?

    (c) is it traceable?   (d) what is its independence number $\alpha(G)$?

    As always, be sure to (briefly) justify your answers.

2. For the graph $G = K_{3,3}$, determine:

    (a) is it Eulerian?   (b) is it Hamiltonian?

    (c) is it traceable?   (d) what is its independence number $\alpha(G)$?

    As always, be sure to (briefly) justify your answers.

3. Find the connectivity and the independence number of the Petersen graph.

    Make sure to prove your answers!

4. Let G be a graph. Prove that the line graph $L(G)$ is claw-free.

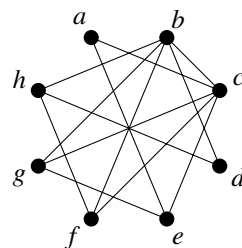5. Let G be a K_3-free graph. Prove that its complement, $\overline{G}$ is claw-free.

    (**Note**: don't misread that: it says K_3, not $K_{3,3}$. And recall $K_3 = C_3$, just three vertices and three edges. So we're saying G doesn't contain induced subgraphs isomorphic to C_3.)

6. Find planar representations of each of the following graphs:

(a):

(b):

14
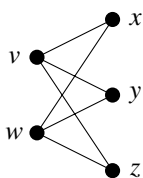
7. Let G be a planar graph, and let $e \in E(G)$. Suppose that in some planar representation of G, the edge e does *not* bound a region. Prove that e is a bridge.

   (**Suggestion**: If the same region R is on both sides of e, what happens if you draw a curve through R from one side of e to the other side?)

8. Prove that there exist planar graphs G_1 and G_2 that have the same number n of vertices, the same number q of edges, and the same number r of regions, **but** which are not isomorphic.

   That is, write down the two graphs, compute the numbers n, q, r for each and verify they match, and then prove that G_1 and G_2 are *not* isomorphic.

Assignment 8: Regular and bipartite graphs; chromatic number

Due by 12:55pm, eastern, on Thursday (tentative), Sept ??
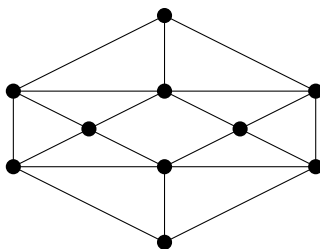

Suggested readings for this problem set:

- Sections 1.5.2–1.5.4, 1.6.1 ,
- and start 1.6.2

All readings are from Harris, Hirst, and Mossinghoff, *Combinatorics and Graph Theory*.

Assignment: due Thursday (tentative), Sept ??, 12:55pm, via Gradescope (VD5BZK):

1. Let G be a connected planar graph of order 24, and suppose that G is regular of degree 3. How many regions are there in a planar representation of G?

2. Let G be a connected planar graph of order $n \geq 3$, and suppose that G is K_3-free. (That is, G has no cycles of length 3.) Prove that the number q of edges of G satisfies $q \leq 2n - 4$.

3. Let G be a bipartite planar graph. Prove that $\delta(G) \leq 3$.

   (*Suggestion*: suppose not, and use problem 2. Hmm, we never said G was connected.)

4. Let G be of order $n \geq 11$. Prove that at least one of G or $\overline{G}$ is nonplanar.

5. Use Kuratowski's Theorem to prove that the Petersen graph G is nonplanar. More specifically, show that G has a subgraph that is a subdivision of $K_{3,3}$.

6. Determine the chromatic number of the Petersen graph. As always, don't forget to justify your answer.

7. Determine the chromatic number of the Birkhoff Diamond, shown below. As always, don't forget to justify your answer.

8. Let G be a graph, let $e \in E(G)$, and let $G' = G - e$. Prove that $\chi(G') \leq \chi(G) \leq \chi(G') + 1$.

Assignment 9: Chromatic polynomial

Due by 12:55pm, eastern, on Thursday (tentative), Sept ??

Suggested readings for this problem set:

- <mark>Sections 1.6.2–1.6.4, 1.7.1</mark> ,
- and start 1.7.2.

All readings are from Harris, Hirst, and Mossinghoff, *Combinatorics and Graph Theory*.

Assignment: due Thursday (tentative), Sept ??, 12:55pm, via Gradescope (VD5BZK):

1. For any integer $n \geq 2$, prove that the only graph G of order n for which $\chi(G) = n$ is the complete graph K_n.

   That is, prove that for any $n \geq 2$ and any graph G of order n, we have $\chi(G) = n$ if and only if G is complete.

2. Recall that $\alpha(G)$ and $\chi(G)$ are the independence number and chromatic number of G, respectively. Prove that for any $n \geq 1$ and any graph G of order n, we have

$$\frac{n}{\alpha(G)} \leq \chi(G) \leq n + 1 - \alpha(G).$$

3. Prove that for any tree T of order n, the chromatic polynomial of T is $c_T(k) = k(k-1)^{n-1}$.

   (*Suggestion*: Use Theorem 1.48 and induction on n.)

4. Prove that for any $n \geq 3$, the chromatic polynomial of the cycle graph C_n is $c_{C_n}(k) = (k-1)((k-1)^{n-1} + (-1)^n)$.

   (*Suggestion*: Use the result of Problem 3 above, Theorem 1.48, and induction on n.)

5. Let $n \geq 2$, and let e be any edge of the complete graph K_n. Prove that K_n/e is isomorphic to K_{n-1}.

6. For any $n \geq 2$, let $H = K_n - e$ be the graph K_n with one edge removed. Prove that the chromatic polynomial of H is is $c_H(k) = k(k-1)\cdots(k-n+3)(k-n+2)^2$.

   (*Suggestion*: Don't use induction. Instead, use the result of Problem 5 above, Theorem 1.48, and the known formula for the chromatic polynomial of K_n.)

7. Prove that the following graph G has no perfect matching.
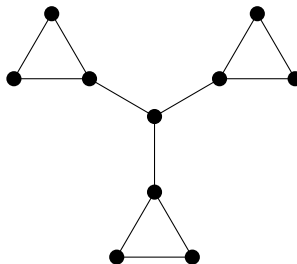
8. (a) Find a perfect matching of C_{12}.

   (b) Find the minimum size of a maximal matching of C_{12}. That is, find a maximal matching M of C_{12} that has some number m of edges, and then prove that any *other* matching M' with $m-1$ or fewer edges cannot be maximal.

Midterm 2 study guide

Content: The questions will all be either

1. Definitions,

2. homework problems,

3. suggested problems,

4. problems we worked in class, or

5. minor variations of one of these.

Problems with very long proofs or that involved some unusual trick will not be on the exam.

You are allowed to use any previous problem from class or from the homework (e.g., "additivity of divisibility" or "the 2 out of 3 rule") on the exam without reproving it, unless otherwise noted on the exam. (E.g., if I ask you to prove "additivity of divisibility" on the exam, you will need to prove this using only the definition of divisibility, and I will remind you of this in the statement of the problem.)

Assignment 10: Matchings; Hall's theorem

*Due by 12:55pm, eastern, on Thursday (tentative), Sept ??*

Suggested readings for this problem set:

- Textbook Sections 1.7.2, 1.7.4 ,

- and start 1.8.1.

All readings are from Harris, Hirst, and Mossinghoff, *Combinatorics and Graph Theory*.

Assignment: due Thursday (tentative), Sept ??, 12:55pm, via Gradescope (VD5BZK):

1. For each of the following graphs, with matchings M as shaded, find an M-augmenting path, and use it to obtain a bigger matching.


   (a)   (b)
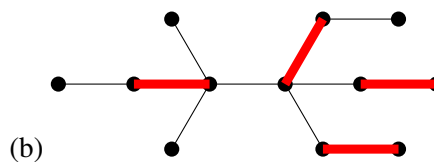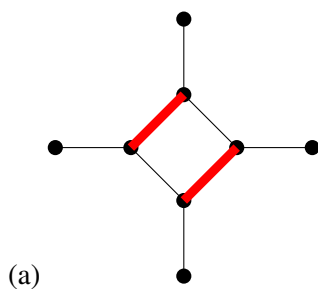
2. For each of the following families of sets, explicitly and carefully check whether the conditions of Theorem 1.52 are met. If so, then find an SDR, saying exactly which element is chosen from each set. If not, then show how the hypotheses are violated.

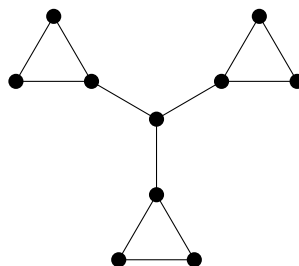   (a) $\{1, 2, 3\}, \{2, 3, 4\}, \{3, 4, 5\}, \{4, 5\}, \{1, 2, 5\}$

   (b) $\{1, 2, 4\}, \{2, 4\}, \{2, 3\}, \{1, 2, 3\}$

   (d) $\{1, 2, 5\}, \{1, 5\}, \{1, 2\}, \{2, 5\}$

3. Use Hall's Theorem to prove that the following bipartite graph does not have a perfect matching.
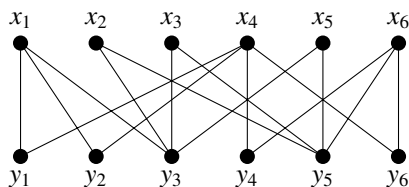
4. Find a maximum matching of the following graph G, and prove that it is indeed a *maximum* matching.

5. Find and draw a connected, 3-regular graph that has both a cut vertex and a perfect matching.

   Don't forget to (briefly) verify that your graph has all these properties. (3-regular, has a cut vertex, and has a perfect matching.)

6. Let G be a graph with connected components $H_1, \ldots, H_k$. Prove that G has a perfect matching if and only if every component H_i has a perfect matching.

7. Let T be a tree. Prove that T has at most one perfect matching.

   (*Suggestion*: Use strong induction on the number of vertices.)

Assignment 11: Ramsey Theory

*Due by 12:55pm, eastern, on Thursday (tentative)[, Sept ??*

Suggested readings for this problem set:

- Sections 1.8.1–1.8.3

All readings are from Harris, Hirst, and Mossinghoff, *Combinatorics and Graph Theory*.

Assignment: due Thursday (tentative), Sept ??, 12:55pm, via Gradescope (VD5BZK):

1. Find and prove a formula for the number of 2-colorings of the edges of K_n, for each $n \geq 1$.

2. Give a full proof that for any integer $k \geq 2$, we have $R(2, k) = k$.

3. Give a full proof that for any integers $p, q \geq 2$, we have $R(p, q) = R(q, p)$.

4. Prove that the following graph G of order 8 satisfies $\omega(G) \leq 2$ and $\omega(\overline{G}) \leq 3$. (That is, prove there are no K_3's in G, and no K_4's in $\overline{G}$.)
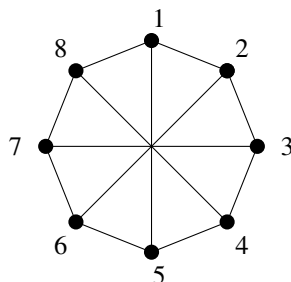
[**Note**: This is a variant of Figure 1.126, which the book points to but skips the analysis of in proving Theorem 1.62. It may help to note that each vertex i has edges to $i - 1$, $i + 1$, and $i + 4$, if we consider these integers modulo 8.]

5. Consider the graph G on 13 vertices $\{1, 2, \ldots, 13\}$ where each vertex i has four edges, connecting it to the vertices $i - 1$, $i + 1$, $i - 5$, and $i + 5$, where we consider these integers modulo 13. (See Figure 1.131 in the textbook.)

   Prove that $\omega(G) \leq 2$.

6. Let G be the graph on 13 vertices from Problem 5 above.

   (a) Prove that for any vertex j, there is no subgraph of $\overline{G}$ that contains vertices j and $j + 3$ and is a copy of K_5. (As before, consider $j + 3$ modulo 13.)

   (b) Prove that for any vertex j, there is no subgraph of $\overline{G}$ that contains vertices j and $j + 6$ and is a copy of K_5. (As before, consider $j + 6$ modulo 13. You may use the result of part (a).)

   (c) Use the results of parts (a) and (b) to prove that $\omega(\overline{G}) \leq 4$.

7. Use Theorem 1.64 and the results of Problems 5 and 6 to prove that $R(3, 5) = 14$.

Final exam study guide

Final exam is **May 13**, 9-11am, in SMUD 014.

The **last day of class** is Tuesday, May 7.

There will be **office hours** before the exam. I will send out a survey to find a time that works for everyone who is planning to attend.

The final exam will be comprehensive.
The exam will be, roughly 8-10 questions, with multiple parts. Some questions will be "prove or disprove". For disproofs, please write out a counterexample as your disproof.

Content: The questions will all be either

1. Definitions,

2. homework problems,

3. suggested problems,

4. problems we worked in class, or

5. minor variations of one of these.

Problems with very long proofs or that involved some unusual trick will not be on the exam.

You are allowed to use any previous problem from class or from the homework (e.g., "additivity of divisibility" or "the 2 out of 3 rule") on the exam without reproving it, unless otherwise noted on the exam. (E.g., if I ask you to prove "additivity of divisibility" on the exam, you will need to prove this using only the definition of divisibility, and I will remind you of this in the statement of the problem.)

Some problems will be calculations, e.g., compute 2^{100} mod 11, or gcd(12345, 67890). Some will be proofs of basic properties (like additivity of transitivity of divisibility, or Euclid's lemma). Most of the problems won't be very long (e.g., I will not ask you to paramaterize pythagorean triples), but I might include one medium length proof (like the infinitude of primes).

A typical exam will have one or two questions from each week of the course (with more emphasis on material since the most recent exam). You can expect problems about (a subset of) the following:

- Definitions (e.g., the definition of a divides b)

- Divisibility

- GCD and LCM

- Euclidean Algorithm

- Linear Equations

- Prime numbers

- Modular arithmetic

- Modular linear equations

- Solving congruence equations

- Inverses

- Fermat's little theorem

- Euler's theorem

- Order

- $\phi(n)$

- Computations involving powers

- Fast squaring

- Polynomials mod p

- Wilson's theorem.

- Quadratic reciprocity

- Primitive roots

TWO problems will be to state and prove two of the following theorems from class (your choice):

- Infinitude of the primes.

- Linear equation theorem (about when the linear equation $ax = b \mod n$ has a solution, and how many solutionts it has).

- Linear combination theorem ($ax + by = n$ has a solution if and only if $n \mid \gcd(a, b)$).

- Fundamental Theorem of Arithmetic.

- Fermat's little theorem

- Euler's theorem

- Wilson's theorem.

- Chinese remainder theorem.

- Let $\gcd(a, n) = 1$. Prove that $a^k \equiv 1 \mod n$ if and only if $o_n(a) \mid k$.

- Prove that primitive roots don't exist mod n if $n = 4p$.

- Euler's formula for $\left(\dfrac{a}{p}\right)$.

- State formula for $\left(\dfrac{-1}{p}\right)$ (the one with two cases) and prove that it is correct.