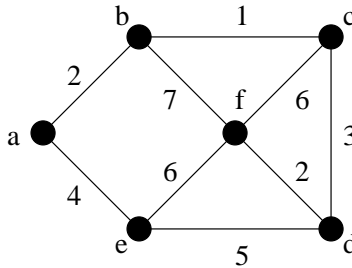


Answers to review problems for final exam

1. In the graph shown below, with edge lengths as indicated, find:  
 (a) the length of the shortest path from vertex  $a$  to each of the other vertices;  
 (b) the shortest path from vertex  $a$  to vertex  $f$ .

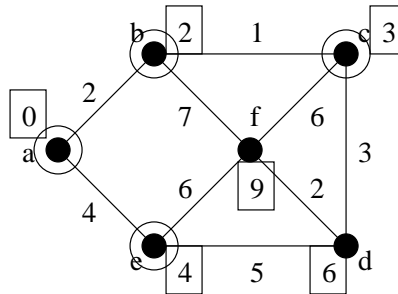


(a)

vertex	$b$	$c$	$d$	$e$	$f$
distance from $a$	2	3	6	4	8

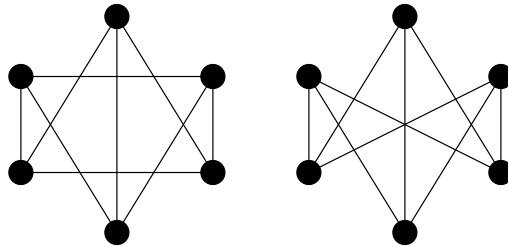
(b)  $abcdf$

2. For the graph in problem 1, Dijkstra's algorithm after four steps finds the neighborhood  $\{a, b, c, e\}$  of vertex  $a$ , with distance labels as shown in the rectangular boxes below. Which vertex gets added to the neighborhood at the next step, and what are the new labels afterwards?



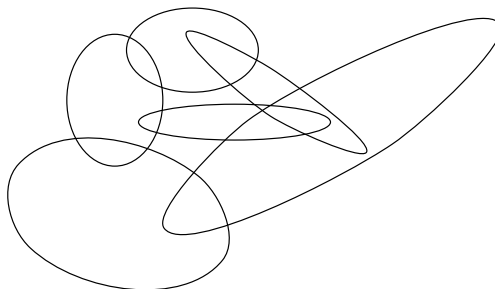
Next added is  $d$ ; label on  $f$  gets updated to 8.

3. Either exhibit an isomorphism between the two graphs shown below, or prove that none exists.

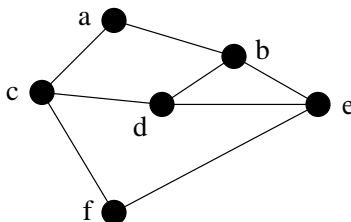


Not isomorphic. The first graph contains some 3-cycles. The second is isomorphic to  $K_{3,3}$  since every vertex in the upper half has an edge to every vertex in the lower half. But  $K_{3,3}$  has no odd cycles.

4. Let  $G$  be the graph whose vertices are the ovals the figure below, with edges representing pairs of ovals that overlap. Write down an adjacency matrix for  $G$ , and draw a picture of  $G$  with vertices and edges shown in the usual way.



Here's the graph, with vertices located approximately at the centers of their corresponding ovals.



Its adjacency matrix is

	$a$	$b$	$c$	$d$	$e$	$f$
$a$	0	1	1	0	0	0
$b$	1	0	0	1	1	0
$c$	1	0	0	1	0	1
$d$	0	1	1	0	1	0
$e$	0	1	0	1	0	1
$f$	0	0	1	0	1	0

5. Prove that a graph with 9 vertices and 14 edges must have a vertex of degree at least 4.

With 14 edges there are  $2 \cdot 14 = 28$  total endpoints of edges. By the pigeonhole principle, some vertex must be an endpoint of at least  $\lceil 28/9 \rceil = 4$  edges.

6. Suppose that each pair of people in a group are either friends, enemies or strangers. Prove that if there are 17 people in the group then there are either three mutual friends, three mutual enemies, or three mutual strangers.

Pick out one person  $x$ . Each of the other 16 people is either friend, enemy or stranger to  $x$ . By the pigeonhole principle, at least 6 others must fall into one of these categories. Suppose that  $x$  has 6 friends in the group. If two friends of  $x$  are friends of each other, we have found three mutual friends. Otherwise, the six friends of  $x$  are all enemies or strangers to each other. Since  $R(3, 3) = 6$ , among them must be three mutual enemies or three mutual strangers.

By similar reasoning, the result holds true if  $x$  has 6 enemies or if there are 6 strangers to  $x$ , so it holds in every case.

7. How many ways are there to assign 8 different tasks to 12 workers if each worker can only do one task? What if each worker can do any number of tasks?

If each can do one task, we are counting 8-permutations of the 12 workers, so there are  $(12)_8$  ways. If each can do any number of tasks, we are counting arbitrary functions from tasks to workers, and there are  $12^8$  ways.

8. Prove the identity

$$\binom{n}{j, k, n-j-k} = \binom{n}{j} \binom{n-j}{k}$$

(a) algebraically, and (b) combinatorially.

(a) Using the formulas, just verify that

$$\frac{n!}{j!k!(n-j-k)!} = \frac{n!}{j!(n-j)!} \cdot \frac{(n-j)!}{k!(n-j-k)!}.$$

(b) The left hand side counts ways to split a set  $X$  of size  $|X| = n$  into disjoint subsets  $A$ ,  $B$ ,  $C$  of sizes  $|A| = j$ ,  $|B| = k$ ,  $|C| = n - j - k$ . We can do this by first choosing  $A$  in  $\binom{n}{j}$  ways, then choosing  $B$  as a subset of  $X \setminus A$  in  $\binom{n-j}{k}$  ways, giving the right hand side.

9. How many different graphs are there with 10 edges and vertex set  $\{1, 2, 3, 4, 5, 6, 7, 8\}$ ? In this problem, graphs count as different if they have different edges, even if they are isomorphic.

The edge set is a 10-element subset of the set of edges of  $K_8$ . Since  $K_8$  has  $\binom{8}{2} = 28$  edges, there are  $\binom{28}{10}$  ways to choose a 10-element subset.

10. How many possible selections of two dozen jelly beans are there if they come in 5 flavors: cherry, lemon, chocolate, blueberry, and mint? How many if you dislike mint and will not take more than three mint jelly beans?

Without the restriction, there are  $\binom{5+24-1}{24}$  selections. If we require at least 4 mint jelly beans, the problem is to select the other 20 jelly beans, in  $\binom{5+20-1}{20}$  ways. Subtract this from the total to get

$$\binom{5+24-1}{24} - \binom{5+20-1}{20}$$

selections with 3 or fewer mint jelly beans.

11. How many 7-permutations of the 26 letters of the alphabet contain the letters  $A, B, C$

(a) in order, but not necessarily consecutively?

(b) in order and consecutively?

(a) Choose positions for  $A, B, C$  in  $\binom{7}{3}$  ways, then fill in with a 4-permutation of the remaining 23 letters, to get

$$\binom{7}{3} (23)_4.$$

(b) If  $ABC$  must occur as a block, there are only 5 choices for the position of this block, instead of  $\binom{7}{3}$ . After placing the  $ABC$  block we again have 4 positions and 23 other letters, giving

$$5 \cdot (23)_4.$$

12. Find all the smaller lists that get merged at every level of recursion when the merge-sort algorithm is used to sort the list of integers

$$(9, 4, 5, 2, 12, 10, 7, 8, 6, 11, 3, 1)$$

(4) and (5) giving (4, 5); (9) and (4, 5) giving (4, 5, 9); (10) and (12) giving (10, 12); (2) and (10, 12) giving (2, 10, 12); (4, 5, 9) and (2, 10, 12) giving (2, 4, 5, 9, 10, 12); (8) and (6) giving (6, 8); (7) and (6, 8) giving (6, 7, 8); (3) and (1) giving (1, 3); (11) and (1, 3) giving (1, 3, 11); (6, 7, 8) and (1, 3, 11) giving (1, 3, 6, 7, 8, 11); finally (2, 4, 5, 9, 10, 12) and (1, 3, 6, 7, 8, 11) giving (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12).

13. Let  $f_k$  denote the  $k$ -th Fibonacci number. Prove that

$$f_1 + f_3 + \cdots + f_{2n-1} = f_{2n}$$

for every positive integer  $n$ .

Proof by induction on  $n$ . Since  $f_1 = f_2 = 1$ , the theorem is true for  $n = 1$ . For  $n > 1$ , we can assume by induction that  $f_{2n-2} = f_1 + f_3 + \cdots + f_{2n-3}$ . Substituting this into the defining recurrence  $f_{2n} = f_{2n-2} + f_{2n-1}$  gives the desired formula.

14. What is wrong with this “proof” that all horses are the same color?

Let  $P(n)$  be the proposition that in every set of  $n$  horses, all the horses are the same color. We will prove  $P(n)$  by induction on  $n$ .

Basis step: Clearly,  $P(1)$  is true.

Induction step: For  $n > 1$ , let  $\{H_1, \dots, H_n\}$  be a set of  $n$  horses. Since  $\{H_1, \dots, H_{n-1}\}$  is a set of  $n - 1$  horses, we may assume by induction that horses  $H_1$  through  $H_{n-1}$  are all the same color. Since  $\{H_2, \dots, H_n\}$  is also a set of  $n - 1$  horses, we may further assume that horses  $H_2$  through  $H_n$  are all the same color. Therefore horse  $H_n$  is the same color as horses  $H_1$  through  $H_{n-1}$ , and all the horses in our set are the same color.

The basis step is correct. In the induction step it is implicitly assumed that the two sets of horses  $\{H_1, \dots, H_{n-1}\}$  and  $\{H_2, \dots, H_n\}$  overlap. But that is false for  $n = 2$ .

15. (a) Let  $p/q$  be a rational number,  $0 < p/q < 1$ . Show that if  $n$  is the smallest positive integer such that  $1/n \leq p/q$ , then  $(p/q) - (1/n)$  is either equal to zero or to a rational number  $p'/q'$  with  $p' < p$ .

(b) Use part (a) and strong induction on  $p$  to prove that every rational number  $p/q$  with  $0 < p/q < 1$  can be expressed as a sum of one or more fractions of the form  $1/n$ . (For example,  $\frac{13}{15} = \frac{1}{2} + \frac{1}{3} + \frac{1}{30}$ .)

(a) The inequality  $1/n \leq p/q$  is equivalent to  $n \geq q/p$ , so the smallest  $n$  is  $\lceil q/p \rceil$ , which is equal to  $(q/p) + x$  for some  $0 \leq x < 1$ . We have  $(p/q) - (1/n) = (np - q)/qn = xp/qn$ . If  $x = 0$ , then  $(p/q) - (1/n) = 0$ . Otherwise,  $(p/q) - (1/n) = p'/q'$  with  $p' = xp$  and  $q' = qn$ . Since  $x < 1$ , we have  $p' < p$ .

(b) Choose  $n$  as in part (a). If  $(p/q) - (1/n) = 0$ , then  $p/q = 1/n$ . Otherwise,  $(p/q) = (1/n) + (p'/q')$  with  $p' < p$ . We can assume by induction that  $p'/q'$  can be expressed as a sum of fractions of the form  $1/m$ . Adding  $1/n$  to such an expression gives one for  $p/q$ .

16. For the 3-error correcting Reed-Solomon code over  $\mathbb{Z}_{11}$  with 4 message symbols and 10 code symbols, determine whether each of the two vectors below is a code vector or not.

(a)  $[2 \ 3 \ 3 \ 1 \ 7 \ 9 \ 6 \ 8 \ 3 \ 1]$

(b)  $[2 \ 3 \ 4 \ 6 \ 7 \ 9 \ 0 \ 8 \ 3 \ 1]$

Since a code vector is the sequence of values of a polynomial of degree  $< 4$ , its fourth difference is zero. Computing fourth differences (mod 11) of each vector above, we find

$$\begin{aligned}\Delta^4 [2 \ 3 \ 3 \ 1 \ 7 \ 9 \ 6 \ 8 \ 3 \ 1] &= [0 \ 0 \ 0 \ 0 \ 0 \ 0], \\ \Delta^4 [2 \ 3 \ 4 \ 6 \ 7 \ 9 \ 0 \ 8 \ 3 \ 1] &= [8 \ 4 \ 8 \ 7 \ 8 \ 2]\end{aligned}$$

The first vector is a code vector and the second is not. Better yet, observe that the second vector has hamming distance 3 from the first vector. Therefore, as soon as we find that the first vector is a code vector, we know that the second vector is not.

17. Consider the linear code over  $\mathbb{Z}_2$  with 4 message bits, 8 code bits, and code matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

- (a) How many errors can this code correct?
- (b) How many errors can it detect?

By examining all sums of rows, we find that every code vector has weight at least 4. Therefore the code can correct 1 error and detect 2 errors.

18. Find all solutions of the system of equations

$$\begin{aligned}4x + 2y + 3z &\equiv 2 \pmod{5} \\ 3x - 2y - z &\equiv 4 \pmod{5}\end{aligned}$$

Using row operations, convert the matrix equation

$$\begin{bmatrix} 4 & 2 & 3 \\ 3 & -2 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 4 \end{bmatrix}$$

to the equivalent equation

$$\begin{bmatrix} 1 & 4 & 4 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \equiv \begin{bmatrix} 3 \\ 0 \end{bmatrix}.$$

We can take  $z$  as a free variable, and then the solution is  $y \equiv -2z \pmod{5}$ ,  $x \equiv y + z + 3 \equiv 3 - z \pmod{5}$ .

19. Find all solutions of the system of equations

$$\begin{aligned}x &\equiv 3 \pmod{5} \\ x &\equiv 1 \pmod{7} \\ x &\equiv 3 \pmod{11}\end{aligned}$$

By the Chinese remainder theorem, there is a unique solution modulo  $5 \cdot 7 \cdot 11 = 385$ . To find it, start with the basic solutions.

$$\begin{aligned}x_1 &\equiv 1 \pmod{5} \\ x_1 &\equiv 0 \pmod{7} \\ x_1 &\equiv 0 \pmod{11}\end{aligned}$$

gives  $x_1 \equiv 77 \cdot 3 = 231 \pmod{385}$ .

$$x_2 \equiv 0 \pmod{5}$$

$$x_2 \equiv 1 \pmod{7}$$

$$x_2 \equiv 0 \pmod{11}$$

gives  $x_2 \equiv 55 \cdot -1 = -55 \pmod{385}$ .

$$x_3 \equiv 0 \pmod{5}$$

$$x_3 \equiv 0 \pmod{7}$$

$$x_3 \equiv 1 \pmod{11}$$

gives  $x_3 \equiv 35 \cdot 6 = 210 \pmod{385}$ . The solution to the given problem is then

$$x \equiv 3x_1 + x_2 + 3x_3 \equiv 113 \pmod{385}.$$

*For the next two problems you will need a calculator. Exam questions on these topics will not require one.*

20. Consider the RSA cryptosystem with public key

$$n = 572149,$$

$$e = 5.$$

(a) Encrypt the message  $x = 339412$  using this cryptosystem.

(b) Given the prime factorization  $n = 727 \cdot 787$ , find the decryption key for this cryptosystem.

(a) Compute  $x^5 \pmod{n}$  to be 470833.

(b) We have  $(p-1)(q-1) = 726 \cdot 786 = 570636$ . The decryption key is the inverse of 5  $\pmod{570636}$ , namely  $d = 456509$ .

21. Use Pollard's "tail-chasing" method to find the prime factorization of  $n$  in the previous problem without knowing it in advance.

Try the simplest choices: take  $x_0 = y_0 = 1$  and use  $x_{k+1} = f(x_k)$ ,  $y_{k+1} = f(f(y_k))$ , with  $f(x) = x^2 + 1 \pmod{572149}$ . Computing  $\gcd(y_k - x_k, n)$  at each step, we find after 28 steps  $y_{28} \equiv 361898$ ,  $x_{28} \equiv 399702$ , and  $\gcd(y_{28} - x_{28}, n) = 727$ .

22. Apply Fermat's test to  $n = 35$ , first using the base 6, then using the base 7. What can be deduced from the result of each test about whether 35 is prime or composite, without using other information?

Compute  $6^{34} \equiv 1 \pmod{35}$ . With this base, 35 passes Fermat's test and may or may not be prime. Next compute  $7^{34} \equiv 14 \pmod{35}$ . With this base, 35 fails Fermat's test, proving that 35 is composite.

23. Repeat the previous problem using Miller's test instead of Fermat's test.

Compute  $6^{17} \equiv 6 \pmod{35}$  and  $6^{34} \equiv 1 \pmod{35}$ . Since  $6 \not\equiv -1 \pmod{35}$ , we see that 35 fails Miller's test, proving that 35 is composite. Of course 35 also fails Miller's test with the base 7, since it fails Fermat's test.

24. Solve the congruence  $7x \equiv 11 \pmod{26}$ .

Using the Euclidean algorithm, compute  $7^{-1} \equiv 15 \pmod{26}$ . Then  $x \equiv 7^{-1} \cdot 11 \equiv 9 \pmod{26}$ .

25. Use Fermat's little theorem to find the inverse of 5 (mod 17).

Since 17 is prime, by Fermat's little theorem,  $5^{16} \equiv 1 \pmod{17}$ , and therefore  $5^{-1} \equiv 5^{15} \pmod{17}$ . Now compute  $5^2 \equiv 8$ ,  $5^4 \equiv 8^2 \equiv 13$ ,  $5^5 \equiv 5 \cdot 13 \equiv 14$ ,  $5^{10} \equiv 14^2 \equiv 9$ , and finally  $5^{15} \equiv 14 \cdot 9 \equiv 7 \pmod{17}$ .

26. Find all solutions of the congruence  $x^2 \equiv 16 \pmod{105}$ . Note that  $105 = 3 \cdot 5 \cdot 7$ .

First find all solutions modulo each prime factor:  $x \equiv \pm 4 \equiv \pm 1 \pmod{3}$ ,  $x \equiv \pm 4 \equiv \mp 1 \pmod{5}$ , and  $x \equiv \pm 4 \pmod{7}$ . There are eight choices of  $\pm$  signs, giving eight solutions (mod 105). Using the Chinese remainder theorem, we find after some work that these are

$$x \equiv \pm 4, \quad x \equiv \pm 46, \quad x \equiv \pm 11, \quad x \equiv \pm 31 \pmod{105}.$$

27. Prove that  $\log_2(3)$  is irrational. Hint: if  $\log_2(3) = p/q$ , then  $2^p = 3^q$ .

Clearly  $\log_2(3)$  is positive, so if it is rational, then it is equal to  $p/q$  for some positive integers  $p$  and  $q$ . Following the hint, this would imply  $2^{p/q} = 3$ , and therefore  $2^p = 3^q$ . This contradicts the uniqueness of prime factorization.

28. Determine whether each of the following functions is  $O(n^2)$ ,  $\Omega(n^2)$ ,  $\Theta(n^2)$ , or none of these.

(a)  $f(n) = \binom{n}{2}$

(b)  $f(n) = n \log n$

(c)  $f(n) = n^2 \log n$

(d)  $f(n) = \begin{cases} n^3 & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even} \end{cases}$

(a) is  $\Theta(n^2)$ , hence also  $O(n^2)$  and  $\Omega(n^2)$ .

(b) is  $O(n^2)$  but not  $\Theta(n^2)$  or  $\Omega(n^2)$ .

(c) is  $\Omega(n^2)$  but not  $\Theta(n^2)$  or  $O(n^2)$ .

(d) is not  $O(n^2)$  or  $\Omega(n^2)$  or  $\Theta(n^2)$ .