CS 70 Discrete Mathematics and Probability Theory
Summer 2019 James Hulett and Elizabeth Yang

HW 2

1 Short Answer: Graphs

(a) (4 Points) Bob removed a degree 3 node in an n-vertex tree, how many connected components are in the resulting graph? (An expression that may contain n.)

(b) (4 Points) Given an n-vertex tree, Bob added 10 edges to it, then Alice removed 5 edges and the resulting graph has 3 connected components. How many edges must be removed to remove all cycles in the resulting graph? (An expression that may contain n.)

(c) (4 Points) True or False: For all $n \geq 3$, the complete graph on n vertices, K_n has more edges than the n-dimensional hypercube. Justify your answer.

(d) (4 Points) A complete graph with n vertices where n is an odd prime can have all its edges covered with x edge-disjoint Hamiltonian cycles (a Hamiltonian cycle is a cycle where each vertex appears exactly once). What is the number, x, of such cycles required to cover the a complete graph? (Answer should be an expression that depends on n.)

(e) (4 Points) Give a set of edge-disjoint Hamiltonian cycles that covers the edges of K_5, the complete graph on 5 vertices. (Each path should be a sequence (or list) of edges in K_5, where an edge is written as a pair of vertices from the set $\{0,1,2,3,4\}$ - e.g: $(0,1),(1,2)$.)

Solution:

(a) **3**.
Each neighbor must be in a different connected component. This follows from a tree having a unique path between each neighbor in the tree as it is acyclic. The removed vertex broke that path, so each neighbor is in a separate component. Moreover, every other node is connected to one of the neighbors as every other vertex has a path to the removed node which must go through a neighbor.

(b) **7**
The problem is asking you to make each component into a tree. The components should have $n_1 - 1$, $n_2 - 1$ and $n_3 - 1$ edges each or a total of $n - 3$ edges. The total number of edges after Bob and Alice did their work was $n - 1 + 10 - 5 = n + 4$, thus one needs to remove 7 edges to ensure there are no cycles.

(c) **False**
This is just an exercise in definitions. The complete graph has $n(n-1)/2$ edges where the hypercube has $n2^{n-1}$ edges. For $n \geq 3$, $2^{n-1} \geq (n-1)/2$.

(d) $(n-1)/2$.

Each cycle removes degree 2 from each vertex. As the degree of each vertex is $n-1$, we require a total of $\frac{n-1}{2}$ disjoint cycles. This is also sufficient. For a construction in the case of n being an odd prime, see explanations below.

(e) $(0,1),(1,2),(2,3),(3,4),(4,0)$
$(0,2),(2,4),(4,1),(1,3),(3,0)$

The following details a procedure for generating the paths using ideas from modular arithmetic. Note that modular arithmetic is not necessary for the solution, but it provides a clean solution.

The idea is that we can generate disjoint Hamiltonian cycles by repeatedly adding an element a to the current node. This produces the sequence of edges $(0,a),(a,2a),\ldots,((p-1)a,0)$ which are disjoint for different a, as long as $a \neq -a \pmod{p}$, as that would simply be subtracting a everytime. (In other words, there exists no integer k such that $-a+pk=a$.)

We use primality to say that inside a sequence the edges are disjoint since the elements $\{0a,\ldots,(p-1)a\}$ are distinct $\pmod{p}$.

2 Bipartite Graph (15 points)

A bipartite graph consists of 2 disjoint sets of vertices (say L and R), such that no 2 vertices in the same set have an edge between them. For example, here is a bipartite graph (with $L =$ {green vertices} and $R =$ {red vertices}), and a non-bipartite graph.

Figure 1: A bipartite graph (left) and a non-bipartite graph (right).

In discussion 02A, we've proved that a graph has no tours of odd length if it is a bipartite. Now, please prove the reversed direction: If undirected G has no tours of odd length, it is a bipartite.

Solution:

Take some vertex v. Add all vertices where the shortest path to v is odd, to R. Add all vertices where the shortest path to v is even, to L. If any of the vertices in $u_1, u_2 \in R$ are adjacent, then we have a tour of odd length formed by appending: the shortest path between v and u_1 (odd), the edge (u_1,u_2) (odd), and the shortest path between u_2 and v (odd). This means no two vertices in R are adjacent. Similarly, if any two vertices $v_1, v_2 \in L$ are adjacent, we get a tour of odd length by appending: the shortest path between v and v_1 (even), the edge (v_1,v_2) (odd), and the shortest path between v_2 and v (even). This means no two vertices in L are adjacent either. If there are

other connected componenets, we can proceed by choosing a new vertex in each component and repeating this process. Then we will have disjoint L, R which include all vertices.

3 Triangulated Planar Graph

In this problem you will prove that every triangulated planar graph (every face has 3 sides; that is, every face has three edges bordering it, including the unbounded face) contains either (1) a vertex of degree 2, 3, 4 (Note that a triangulated planar graph cannot contain a vertex with degree 1; can you think about a reason why?); (2) two degree 5 vertices which are adjacent; or (3) a degree 5 and a degree 6 vertices which are adjacent. We will construct a proof by cases. Note that while we are attempting to prove that the former holds, we are still assuming that the graph can have vertices with degree greater than 6. Please justify your answers.

(a) (5 points) Place a "charge" on each vertex v of value $6 - \text{degree}(v)$. What is the sum of the charges on all the vertices? (*Hint*: Use Euler's formula and the fact that the planar graph is triangulated.)

(b) (5 points) What is the charge of a degree 5 vertex and of a degree 6 vertex?

(c) (5 points) Suppose now that we shift $1/5$ of the charge of a degree 5 vertex to each of its neighbors that has a negative charge. (We refer to this as "discharging" the degree 5 vertex.) After discharging all degree 5 vertices, when would there be a degree 5 vertex with positive remaining charge?

(d) (5 points) If no degree 5 vertices have positive charge after discharging the degree 5 vertices, does there exist any vertex with positive charge after discharging? If there is such a vertex, what are the possible degrees of that vertex?

(e) (5 points) Suppose there exists a degree 7 vertex with positive charge after discharging the degree 5 vertices. How many neighbors of degree 5 might it have?

(f) (5 points) Continuing from Part (e). Since the graph is triangulated, are two of these degree 5 vertices adjacent?

(g) (5 points) Finish the proof from the facts you obtained from the previous parts.

Solution:

(a) Let V be the vertex set , E be the edge set, F be the faces in the graph, we have

$$\sum_{v \in V} 6 - \text{degree}(v) = 6|V| - \sum_{v \in V} \text{degree}(v) \quad (1)$$

$$= 6|V| - 2|E|. \quad (2)$$

The last step is because that we count each edge twice as degree for each end vertex. And since the graph is triangulated, each face uses exactly three edges and each edge is shared by

two faces, so we can substitute $|F| = 2|E|/3$ in Euler's formula to get

$$\begin{aligned} |V| + |F| &= |E| + 2 && (3)\\ |V| + \frac{2|E|}{3} &= |E| + 2 && (4)\\ 3|V| + 2|E| &= 3|E| + 6 && (5)\\ |E| &= 3|V| - 6. && (6) \end{aligned}$$

Substitute (6) into (2) to get that the sum of charge is 12.

(b) The charge is 1 for degree 5 vertex, and 0 for degree 6 vertex.

(c) If there is a degree 5 vertex with positive remaining charge, that means at least one of its neighbors is not negatively charged. In other words, at least one of its neighbors has degree 2, 3, 4, 5, or 6. We omit degree 1, since in a triangulated planar graph, it is not possible to have vertices of degree 1.

(d) Yes, there exists a vertex with positive charge. Since we know that the sum of charge of the entire graph is 12, and that the total charge of the graph remains conserved during 'discharging'; it is impossible to have no positively charged vertex.

The possible degrees of vertex that have positive charge after discharging are $2, 3, 4, 7$. Vertices with degree at least 8 will have initial charge -2, and will not have positive charge even if all their neighbors are of degree 5. We note that in a triangulated planar graph, it is not possible to have vertices of degree 1. // Side note: one can use Part (e) and Part (f) to rule out the possibility of degree-7 vertices. But for simplicity we only require students to rule out degrees 5 and 8 and beyond. The idea is that, we can't have two adjacent degree-5 vertices to have zero-charge after discharging. Suppose that there exists a degree-7 vertex with positive charges after discharging, then by Part(e) and ff) out of the 7 neighbors, 6 of them have to be of degree 5, and two of these degree-5 vertices have to be adjacent, since they need to form triangles with the degree 7 vertex. Therefore, if none of the degree-5 vertices have positive charges, then we get two adjacent degree-5 vertices that have zero-charge, which is a contradiction.

(e) At least 6 out of the 7 are degree 5.

(f) Since the graph is triangulated, observe that fixing a drawing of the planar graph, we can order neighbors of the degree 7 node clockwise. And every two consecutive neighbors (defined by the ordering) form a triangle with the degree 7 vertex. From Part (e) we know that at least 6 out of the 7 are of degree 5. Therefore, it is impossible that none of these degree-5 vertices are adjacent to another degree-5 node.

(g) We split the proof into several cases. First note that there is always a vertex with degree at most 5. Suppose the contrary that every vertex is of degree at least 6, then the total charge would not have been positive, contradicting Part (a), where we showed the total charge is always 12.

If all vertices have degree less than 5, then we see that this is case (1). Therefore we consider the case where there is always a vertex of degree 5 from now on.

When there is a degree-5 vertex with a positive remaining charge, the statement is true by Part (c). When there is no degree-5 vertex with positive remaining charge, we know from Part (d) that either there is a positively charged vertex with degree $2,3,4$ or with degree 7. For a degree-7 vertex, we know that at least two degree 5 vertices are adjacent from Part (f) which concludes our proof.

Side note: alternatively, one could simply rule out the possibility of a degree-7 vertex as explained in Part (d).

4 Modular Exponentiation

Compute the following:

(a) (5 points) $13^{2018} \pmod{12}$

(b) (5 points) $8^{11111} \pmod{9}$

(c) (5 points) $7^{256} \pmod{11}$

(d) (5 points) $3^{160} \pmod{23}$

Solution:

(a) 13 is always 1 mod 12, so 13 to any power mod 12 is 1.

(b) 8 is its own inverse mod 9, therefore, if 8 is raised to an odd power, the number will be 8 mod 9. So the answer is 8.

Also notice that $8 \equiv -1 \pmod{9}$ so $8^{11111} \equiv (-1)^{11111} \equiv -1 \equiv 8 \pmod{9}$. In general, $m-1 \equiv -1 \pmod{m}$, so $m-1$ is always its own inverse. This is a useful trick so you can avoid computing the inverse of $m-1$ by hand. You can also check that $(m-1)^2 \equiv m^2 - 2m + 1 \equiv 1 \pmod{m}$, which is another proof that $m-1$ is its own inverse modulo m.

(c) We can use repeated squaring for this question.

$7^2 \equiv 5 \pmod{11}$

$7^4 \equiv (7^2)^2 \equiv 5^2 \equiv 3 \pmod{11}$

$7^8 \equiv (7^4)^2 \equiv 3^2 \equiv 9 \pmod{11}$

$7^{16} \equiv (7^8)^2 \equiv 9^2 \equiv 4 \pmod{11}$

$7^{32} \equiv (7^{16})^2 \equiv 4^2 \equiv 5 \pmod{11}$

$7^{64} \equiv (7^{32})^2 \equiv 5^2 \equiv 3 \pmod{11}$

$7^{128} \equiv (7^{64})^2 \equiv 3^2 \equiv 9 \pmod{11}$

$7^{256} \equiv (7^{128})^2 \equiv 9^2 \equiv 4 \pmod{11}$

A way to avoid repeated squaring for too many times in both part (c) and part (d) is to use Fermat's Little theorem to simplify the exponent. We can rewrite the exponent to be $256 = (11-1)*25+6$, and this will give us $7^{(10*25+6)} \equiv (7^{10})^{25} * 7^6 \pmod{11} \equiv 1^{25} * 7^6 \pmod{11} \equiv 7^6 \pmod{11}$. From this step, we can easily simplify it into $(7^2)^3 \pmod{11} \equiv 5^3 \pmod{11} \equiv 4 \pmod{11}$.

(d) We can notice that $160 = 128 + 32$, the sum of two powers of two. Then, like the previous part, we can use repeated squaring to compute this problem.

$3^2 \equiv 9 \pmod{23}$

$3^4 \equiv (3^2)^2 \equiv 9^2 \equiv 12 \pmod{23}$

$3^8 \equiv (3^4)^2 \equiv 12^2 \equiv 6 \pmod{23}$

$3^{16} \equiv (3^8)^2 \equiv 6^2 \equiv 13 \pmod{23}$

$3^{32} \equiv (3^{16})^2 \equiv 13^2 \equiv 8 \pmod{23}$

$3^{64} \equiv (3^{32})^2 \equiv 8^2 \equiv 18 \pmod{23}$

$3^{128} \equiv (3^{64})^2 \equiv 18^2 \equiv 2 \pmod{23}$

$3^{160} \equiv (3^{128})(3^{32}) \equiv (2)(8) \equiv 16 \pmod{23}$

Note that in this problem we can also simplify the exponent first like the alternating solution in part (c).

5 Euler's Totient Function

Euler's totient function is defined as follows:

$$\phi(n) = |\{i : 1 \leq i \leq n, \gcd(n,i) = 1\}|$$

In other words, $\phi(n)$ is the total number of positive integers less than or equal to n which are relatively prime to it. Here is a property of Euler's totient function that you can use without proof:

For m, n such that $\gcd(m,n) = 1$, $\phi(mn) = \phi(m) \cdot \phi(n)$.

(a) (5 points) Let p be a prime number. What is $\phi(p)$?

(b) (5 points) Let p be a prime number and k be some positive integer. What is $\phi(p^k)$?

(c) (5 points) Let p be a prime number and a be a positive integer smaller than p. What is $a^{\phi(p)} \pmod{p}$?
(Hint: use Fermat's Little Theorem.)

(d) (5 points) Let b be a positive integer whose prime factors are $p_1, p_2, \ldots, p_k$. We can write $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_k^{\alpha_k}$.

Show that for any a relatively prime to b, the following holds:

$$\forall i \in \{1,2,\ldots,k\},\ a^{\phi(b)} \equiv 1 \pmod{p_i}$$

Solution:

(a) Since p is prime, all the numbers from 1 to $p-1$ are relatively prime to p.

So, $\phi(p) = p-1$.

(b) The only positive integers less than p^k which are not relatively prime to p^k are multiples of p.

Why is this true? This is so because the only possible prime factor which can be shared with p^k is p. Hence, if any number is not relatively prime to p^k, it has to have a prime factor of p which means that it is a multiple of p.

The multiples of p which are $\leq p^k$ are $1 \cdot p, 2 \cdot p, \ldots, p^{k-1} \cdot p$. There are p^{k-1} of these.

The total number of positive integers less than or equal to p^k is p^k.

So $\phi(p^k) = p^k - p^{k-1} = p^{k-1} \cdot (p-1)$.

(c) From Fermat's Little Theorem, and part (a),

$a^{\phi(p)} \equiv a^{p-1} \equiv 1 \pmod{p}$

(d) From the property of the totient function and part (b):

$$\begin{aligned}\phi(b) &= \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_k^{\alpha_k}) \\ &= \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \ldots \phi(p_k^{\alpha_k}) \\ &= p_1^{\alpha_1 - 1}(p_1 - 1) \cdot p_2^{\alpha_2 - 1}(p_2 - 1) \ldots p_k^{\alpha_k - 1}(p_k - 1)\end{aligned}$$

This shows that, for every p_i, which is a prime factor of b, we can write $\phi(b) = c \cdot (p_i - 1)$, where c is some constant. Since a and b are relatively prime, a is also relatively prime with p_i. From Fermat's Little Theorem:

$a^{\phi(b)} \equiv a^{c \cdot (p_i - 1)} \equiv (a^{(p_i - 1)})^c \equiv 1^c \equiv 1 \mod p_i$

Since we picked p_i arbitrarily from the set of prime factors of b, this holds for all such p_i.

6 Just a Little Proof (15 points)

Suppose that p and q are distinct odd primes and a is an integer such that $\gcd(a, pq) = 1$. Prove that $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$.

Solution:

Note: This problem is essentially asking you to prove the correctness of RSA.

We know that a is not a divsible by p and a is not divisible by q since $\gcd(a, pq) = 1$.We subtract a from both sides to get

$$a^{(p-1)(q-1)+1} - a \equiv 0 \pmod{pq}$$
$$a(a^{(p-1)(q-1)} - 1) \equiv 0 \pmod{pq}$$

Since p, q are primes, we just need to show that the left hand side is divisible by both p and q. Since a is not divisible by p, we can use Fermat's Little Theorem to state that $a^{p-1} \equiv 1 \pmod{p}$.

$$a\big((a^{(p-1)})^{q-1} - 1\big) \equiv a(1^{q-1} - 1) \equiv 0 \pmod{p}$$

Thus $a(a^{(p-1)(q-1)} - 1)$ is divisible by p. We can apply the same reasoning to show that the expression is divisible by q. Therefore we have proved our claim that $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$.

Alternative Proof:
Because $\gcd(a, pq) = 1$, we have that a does not divide p and a does not divide q. By Fermat's Little Theorem,

$$a^{(p-1)(q-1)+1} = (a^{(p-1)})^{(q-1)} \cdot a \equiv 1^{q-1} \cdot a \equiv a \pmod{p}.$$

Similarly, by Fermat's Little Theorem, we have

$$a^{(p-1)(q-1)+1} = (a^{(q-1)})^{(p-1)} \cdot a \equiv 1^{p-1} \cdot a \equiv a \pmod{q}.$$

Now, we want to use this information to conclude that $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$. We will first take a detour and show a more general result (you could write this out separately as a lemma if you want).

Consider the system of congruences

$$x \equiv a \pmod{p}$$
$$x \equiv a \pmod{q}.$$

Let's run the CRT symbolically. First off, since p and q are relatively prime, we know there exist integers g, h such that

$$g \cdot p + h \cdot q = 1.$$

We could find these via Euclid's algorithm. By the CRT, the solution to our system of congruences will be

$$x \equiv a \cdot y_1 \cdot q + a \cdot y_2 \cdot p \pmod{pq}.$$

To solve for y_1 and y_2, we must find y_1 such that

$$x_1 \cdot p + y_1 \cdot q = 1$$

and y_2 such that

$$x_2 \cdot q + y_2 \cdot p = 1.$$

This is easy since we already know $g \cdot p + h \cdot q = 1$: the answers are $y_1 = h$ and $y_2 = g$. Finally we can plug in to the solution to get

$$x \equiv a \cdot h \cdot q + a \cdot g \cdot p \equiv a(h \cdot q + g \cdot p) \equiv a \cdot 1 \equiv a \pmod{pq}.$$

Therefore by the CRT we know that the set of solutions that satisfy both $x \equiv a \pmod{p}$ and $x \equiv a \pmod{q}$ is exactly the set of solutions that satisfy $x \equiv a \pmod{pq}$.

So since $a^{(p-1)(q-1)+1} \equiv a \pmod{p}$ and $a^{(p-1)(q-1)+1} \equiv a \pmod{q}$, then by the CRT we know that $a^{(p-1)(q-1)+1}$ satisfies $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$.