CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 03

Due: Saturday, 2/10, 4:00 PM
Grace period until Saturday, 2/10, 6:00 PM

Sundry

Before you start writing your final homework submission, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Short Tree Proofs

Note 5

Let $G = (V, E)$ be an undirected graph with $|V| \geq 1$.

(a) Prove that every connected component in an acyclic graph is a tree.

(b) Suppose G has k connected components. Prove that if G is acyclic, then $|E| = |V| - k$.

(c) Prove that a graph with $|V|$ edges contains a cycle.

2 Touring Hypercube

Note 5

In the lecture, you have seen that if G is a hypercube of dimension n, then

- The vertices of G are the binary strings of length n.
- u and v are connected by an edge if they differ in exactly one bit location.

A *Hamiltonian tour* of a graph is a sequence of vertices $v_0, v_1, \ldots, v_k$ such that:

- Each vertex appears exactly once in the sequence.
- Each pair of consecutive vertices is connected by an edge.
- v_0 and v_k are connected by an edge.

(a) Show that a hypercube has an Eulerian tour if and only if n is even.

(b) Show that every hypercube has a Hamiltonian tour.

1 (a) Every connected component is connected and acyclic, thus a tree.

(b) For each tree $v + 1 = e + 2$ bcs $f = 1$

Thus we have $e = v - 1$ for each component

Summing $\sum^{k} e = |E| = \sum^{k} (v-1) = |V| - k$

gives the total.

(c) We note that acyclic & $|V|-1$ edges means a connected tree. Thus adding any edge would produce a cycle. Thus $|V|$ is cyclic.

2 (a) $2 | \text{degree}(i)$ for $i \in V$ only when n is even, as the vertices have degree n.

(b) Hypothesis: There exist a hamilton tour starting at any vertex and end at any other vertex connected to start.

Base: $n = 1$, true

Inductive step: $n+1$ hypercube.

Apply inductive hypothesis to 0-cube & 1-cube which are hypercubes of dimension 1.

(example)

0-cube: start at 0...0, end at 0...1

1-cube: Start at 10...01, end at 10...0

Connect the two tours by 0...1 to 10...01

Thus, we have a tour starting 0...0 end at 10...0

Why does this prove the induction hypothesis

Note that the hypercube is symmetrical, thus we can choose any start point, and any end point by showing that in case of 0-cube start, we end at the 1-cube connected component. But if we instead categorize by say the x1-cube and the x0 cube we can have 0...0 connected to any point. Thus hypothesis proved.

3 Planarity and Graph Complements

Note 5

Let $G = (V,E)$ be an undirected graph. We define the complement of G as $\overline{G} = (V,\overline{E})$ where $\overline{E} = \{(i,j) \mid i,j \in V, i \neq j\} - E$; that is, $\overline{G}$ has the same set of vertices as G, but an edge e exists is $\overline{G}$ if and only if it does not exist in G.

(a) Suppose G has v vertices and e edges. How many edges does $\overline{G}$ have?

(b) Prove that for any graph with at least 13 vertices, G being planar implies that $\overline{G}$ is non-planar.

(c) Now consider the converse of the previous part, i.e., for any graph G with at least 13 vertices, if $\overline{G}$ is non-planar, then G is planar. Construct a counterexample to show that the converse does not hold.

Hint: Recall that if a graph contains a copy of K_5, then it is non-planar. Can this fact be used to construct a counterexample?

4 Modular Practice

Note 6

Solve the following modular arithmetic equations for x and y.

(a) $9x + 5 \equiv 7 \pmod{13}$.

(b) Show that $3x + 12 \equiv 4 \pmod{21}$ does not have a solution.

(c) The system of simultaneous equations $5x + 4y \equiv 0 \pmod{7}$ and $2x + y \equiv 4 \pmod{7}$.

(d) $13^{2023} \equiv x \pmod{12}$.

(e) $7^{62} \equiv x \pmod{11}$.

5 Short Answer: Modular Arithmetic

Note 6

(a) What is the multiplicative inverse of $n-1$ modulo n? (Your answer should be an expression that may involve n)

(b) What is the solution to the equation $3x \equiv 6 \pmod{17}$?

(c) Let $R_0 = 0; R_1 = 2; R_n = 4R_{n-1} - 3R_{n-2}$ for $n \geq 2$. Is $R_n \equiv 2 \pmod{3}$ for $n \geq 1$? (True or False)

(d) Given that $(7)(53) - m = 1$, what is the solution to $53x + 3 \equiv 10 \pmod{m}$? (Answer should be an expression that is interpreted $\pmod{m}$, and shouldn't consist of fractions.)

3 (a) The complete graph of v vertices has $\frac{v(v-1)}{2}$ edges. So $\bar{e} = \frac{v(v-1)}{2} - e$

(b) G planar $\Rightarrow e \le 3v-6$

$\bar{G}$: $\bar{e} = \frac{v(v-1)}{2} - e \ge \frac{v^2-8v+19}{2}$

For $v = 13$ $\bar{e} \ge 92$

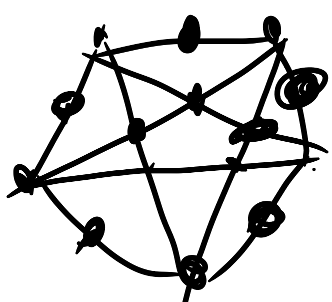
$\bar{e} = 92 \not\le 48-6 = 42$

Thus $\bar{e}$ non-lanar

as $\bar{e}$'s lowerbound grows quadratically while lower bound grows only linearly.

$v \ge 13$, $\bar{G}$ must be nonlinear.

(c)



$\bar{G}$ such as th

$\bar{e} = 2 \cdot 5 + 3 \cdot 5 = 25$

$v = 15$

but $e = \frac{15 \cdot 14}{2} - 25 = 80$

$e = 80 > 3v-8 = 37$

Thus G also non planar

4. (a) $x = 6$

(b) $3x + 8 \equiv 0 \Rightarrow 3x = 21d - 8$

$\underset{\text{mod } 3}{\equiv} 0 \equiv 0 - 8$

$\not\equiv 0$

$3x \quad 16$

Thus no solution

(c) $5x + 4y \equiv 0 \mod 7 \quad 2x + y \equiv 4 \mod 7$

$\Rightarrow 3x \equiv 2 \mod 7 \Rightarrow x \equiv 3 \mod 7$

$\Rightarrow y \equiv 5 \mod 7$

(d) $\Rightarrow \begin{cases} x \equiv 3 \\ y \equiv 5 \end{cases}$

(e) $(49)^{31} \equiv 5^{31} \equiv 25^{15} \cdot 5 \equiv 3^{15} \cdot 5 \equiv 27^5 \cdot 5 \equiv 5^5 \cdot 5 \equiv 25^3 \equiv 27$

$\equiv 5 \mod 11$

5. (a) $(n-1) \mod n \equiv -1$

$1 \equiv 1 - n \mod n$

$m(n-1) \mod n \equiv -m \equiv 1 - n \mod n$

$\Rightarrow m = n - 1 \Rightarrow n-1$ is it's own multiplicative inverse.

(b) $3x \equiv 6 \mod 17 \Rightarrow x_0 = 2$ is a solution

while $\gcd(3, 17) = 1$, and it's multiplicative inverse of 3 is 6. $\Rightarrow 6 \cdot 3x \equiv x \equiv 36 \equiv 2$

Thus $x = 2 + 17d$.

(c) Yes as $R_n \equiv R_{n-1} \mod 3$

while $R_{n-1} \equiv R_{n-2} \cdots \equiv R_0 \equiv 2$

Thus $R_n \equiv 2 \mod 3$

(d)

$7 \cdot 53 = 1 \mod m \Rightarrow 7$ is multiplicative inverse

$53x + 3 \equiv 10 \Rightarrow 53x \equiv 7 \mod m \Rightarrow 7 \cdot 53x \equiv x \equiv 49 \mod m$

bcs $7 \cdot 53 - m = 1 \Rightarrow 49 < m \Rightarrow x \equiv 49 \mod m$

6 Wilson's Theorem

Note 6

Wilson's Theorem states the following is true if and only if p is prime:

$$(p-1)! \equiv -1 \pmod{p}.$$

Prove both directions (it holds if AND only if p is prime).

Hint for the if direction: Consider rearranging the terms in $(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$ to pair up terms with their inverses, when possible. What terms are left unpaired?

Hint for the only if direction: If p is composite, then it has some prime factor q. What can we say about $(p-1)! \pmod{q}$?

If: $p=2$ is exception but for $p>2$, statement holds

Consider $((p-1)!)^2 \bmod p \equiv 1$

why? every $1 \ldots p-1$ has a unique multiplicative inverse

Thus $1 \ldots p-1$ & $1 \ldots p-1$ can each pair up and form 1s.

Thus Suppose $(p-1)! \equiv m$ with $m^2 \equiv 1 \Rightarrow m \equiv -1$ or 1.

We note that $(p-1)^{-1} \equiv p-1 \bmod p$

$(p-1)!\,(p-1) \equiv (p-2)! \equiv 1 \cdot p-1$ or $-1 \cdot p-1 \bmod p$

$\equiv -1$ or 1.

But $(p-2)!$ must be 1 as each member besides 1 is paired up with a different member as inverse unique and mutual, and $m^2 \equiv 1$ only has $m \equiv 1$ or $m \equiv -1 \equiv p-1$ Thus $(p-2)! \equiv 1 \bmod p$

and $(p-1)! \equiv -1 \bmod p$

Only if: $(p-1)! \equiv -1 \Rightarrow (p-2)! \equiv 1$

Thus a partial product $m \mid (p-2)!$ and $n = \frac{(p-2)!}{m}$ form inverse.

but either $\gcd(m,p) \neq 1$ or $\gcd(n,p) \neq 1$

as p's composite must belong to $\{1 \ldots p-1\}$, thus

m or n must not exist inverse $\Rightarrow$ contradictive.

Thus $(p-1)! \not\equiv -1 \bmod p \Rightarrow p$ must be prime.