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) a graph is a tree if it is connected and acyclic.
so every connected component in a acyclic graph is also acyclic, so they are all trees.

(b) tree : $E_1 = V_1 - 1$ one connect component

$E_1 + \dots + E_k = V_1 + \dots V_k - k \Rightarrow |E| = |V| - k$

(c) If it is acyclic, at most have $|V| - k$ edges,
when $k = 1$, $|V| - 1$ edges and all connect,
add one more edge, will be form a cycle.
a connected graph if is not a tree, it contains a cycle

2. (a) Eulerian tour $\Leftrightarrow$ $G$ is even degree and is connect

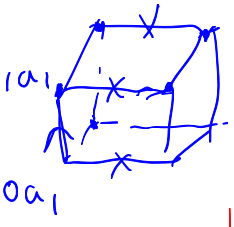
a hypercube's degree is $n$, so $n$ should be even

have a eulerian tour $\Leftrightarrow$

(b) if $n$ is even, have a eulerian tour. is right.

if $n$ is odd, → split it two part → something wrong

$0a_1a_2 \ldots a_{n-1}$ $1a_1a_2 \ldots a_{n-1}$




Yes how to say it?

use ↓ Induction.

$H$ $n+1$ - dimensional hypercube

$H_b$ $n$ - dimensional subcube consisting of those string with inital bit $b$

$H_0 \to H_1$

$x_0 \sim y_0 \sim y_1 \to x_1$

# 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) $\underbrace{n-1+n-2+\ldots\ldots+0}_{n} = \frac{n(n-1)}{2}$

$\frac{V(V-1)}{2} - e$

(b) $V \geq 13$ $\quad e \leq 3V-6$ $\quad V+f = e+2$

$3f \leq 2e \quad 3(e+2-V) \leq 2e$

$e \leq 3V-6$

when $V \geq 13$

$\frac{V(V-1)}{2} \geq \frac{V*12}{2} = 6V$

$e \leq 3V-6$

$\frac{V(V-1)}{2} - e \geq \frac{V(V-1)}{2} - 3V + 6$

$= 3V+6$

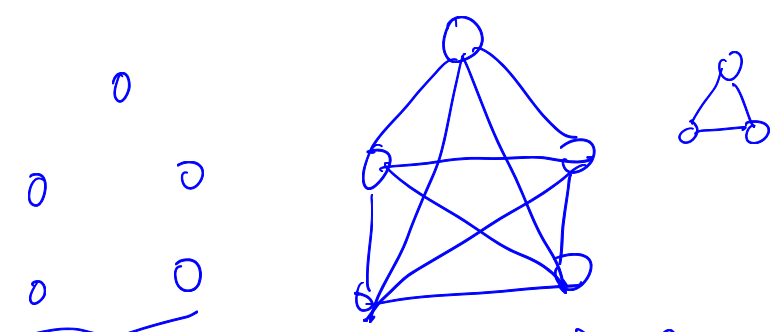
no need

$\frac{V(V-1)}{2} - 3V + 6 \geq 3V-6$

$V^2 - 13V + 24 \geq 0$

(c) $\checkmark$ K5, 5 $\quad V \geq 13$ $\quad E + \bar{E} \geq 2*(3V-6)$

$\bar{G}$



↓ this will be K5, 5 in G

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

$9x \equiv 2 \pmod{13}$

$x \equiv 6 \pmod{13}$

$\gcd(9, 13) = 1$ $\quad 9y \equiv 1 \pmod{13}$

$9 * x + 13 * y = 1$

$13 * 0 + 9 * 1 = 9 \quad \cdots ①$

$(13 * 1) + 9 * 0 = 13 \quad \cdots ②$

$② - ①$ ; $13 * 1 - 9 * 1 = 4 \quad \cdots ③$

$① - 2 * ③$ : $-13 * 2 + 9 * 3 = 1$

$y \equiv 3 \pmod{13}$

(b) $3x + 12 \equiv 4 \pmod{21}$

$\gcd(3, 21) = 3 \neq 1$ . no inverse of $x \pmod{21}$

$4 + 21k \equiv 1 \pmod{3}$

$3x + 12 \neq 1 \pmod{3}$ for every $x$

$3x \equiv 13 \pmod{21} \rightarrow$ ~~$3x = 21k + 13$~~ more direct → impossible

$x = 7k + \frac{13}{3}$

int int not int

(c) $\begin{cases} 5x + 4y \equiv 0 \pmod{7} \quad \cdots ① \\ 2x + y \equiv 4 \pmod{7} \quad \cdots ② \end{cases}$

$4 * ② - ①$ $\quad 3x \equiv 16 \equiv 2 \pmod{7}$

$x \equiv 10 \equiv 3 \pmod{7}$

$3y \equiv 1 \pmod{7}$.

$y \equiv 5 \pmod{7}$

$y \equiv -2 \pmod{7}$

$\equiv 5$

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

$13 \equiv 1 \pmod{12}$ $\quad x = 1$

11 | 27 (2, 2)

6 | 24 (2, 2, 3)

(c) ~~(a)~~ $(14)^{31} \equiv 3^{31} \equiv 3*(3^3)^{10} \equiv 3*(5)^{10}$

$\equiv 3*(25)^5 \equiv 3*3^5 \equiv 3^6 \equiv (27)^2 \equiv 5^2 \equiv 3$

$\pmod{11}$.

5. (a) $x * (n-1) \equiv 1 \pmod n$ $(n-1)$

$x * n - x \equiv 1 \pmod n$ $-x = kn + 1$

$-x \equiv 1 \pmod n \Rightarrow x \equiv n-1 \pmod n$

(b) $3x \equiv 6 \pmod{17}$ $\gcd(3, 17) = 1$.

$3 * 6 - 17 = 1$

$x \equiv 36 \equiv 2 \pmod{17}$

$17 \overline{)36}\ 2$

(c) $R_1 = 2$

$R_2 = 4 * 2 - 3 * 0 = 8$

True Induction.

(d) $53x \equiv 7 \pmod m$ $53y \equiv 1 \pmod m$.

$y = 7$

$x \equiv \frac{49}{14} \pmod m$

?

# 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 $(p-1)! \pmod{q}$?

$(p-1)! \pmod{q} \equiv 0$

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

$k, q \equiv -1 \pmod{p}$