CS 70	Discrete Mathematics and Probability Theory	
Spring 2026	Sinclair, Song	HW 03

Due: Saturday, 2/14, 4:00 PM
Grace period until Saturday, 2/14, 6:00 PM
Remember to show your work for all problems!

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 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 cycle* of a graph (with ≥ 2 vertices) is a cycle that visits every vertex exactly once (except that the start and end vertices are the same).

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

(b) Prove that every hypercube of dimension $n \geq 2$ has a Hamiltonian cycle.

2 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?

3 Modular Practice

Note 6

Solve the following modular arithmetic equations for x and y. For each subpart, show your work and justify your answers.

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

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

4 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 $(p-1)! = 1 \cdot 2 \cdot \dots \cdot (p-1)$ *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 $(p-1)! \pmod{q}$*?*

5 How Many Solutions?

Note 6

Consider the equation $ax \equiv b \pmod{p}$ for prime p. In the below three parts, all values a, b, x are defined as values in the range $\{0, 1, \dots p-1\}$. In addition, include justification for your answers to all the subparts of this problem.

(a) For how many pairs (a, b) does the equation have a unique solution?

(b) For how many pairs (a, b) does the equation have no solution?

(c) For how many pairs (a, b) does the equation have p solutions?

For this last part, consider the equation $ax \equiv b \pmod{pq}$ for distinct primes p, q. All values a, b, x are defined as values in in the range $\{0, 1, \dots pq-1\}$.

(d) If $\gcd(a, pq) = p$, show that there exists a solution if and only if $b = 0 \pmod{p}$. (Hint: Try to relate modular equations to their corresponding algebraic equations, and vice versa.)