CS 135 Spring 2023: Final Exam B

NAME	Humna Sultan
Pledge	I pledge my Honor that I have abided by the Stevens Honor System.

Please write your name on the bluebook also and submit both the exam and the bluebook.

Answer Problems 1 and 2 on the exam sheet directly. For Problem 3 be sure to fill in the table on the exam and show your work in the bluebook.

Problem 1. (20 points) Indicate whether each of the following statements is True or False. All graphs are undirected.

T 1) The number of vertices of odd degree in a graph is always even.

T 2) If there is a walk in a graph from vertex a to vertex b, then there is a path from a to b.

F 3) If an N-vertex graph has an open trail of length N, then the graph contains a cycle

T 4) If every cycle in a graph is of even length, then the graph has a 2-coloring.

F 5) Every connected graph contains a subgraph that is a tree.

T 6) If a connected planar graph has R regions, then it contains at least R distinct cycles.

T 7) Every circuit in a graph is a cycle.

T 8) If there is a circuit that contains vertices a, b, then there is a cycle that contains a and b.

F 9) If a graph has a cycle that contains vertices a and b but not c, and a different cycle that contains b and c but not a, then it contains a cycle that contains a and c.

F 10) If a graph has a cycle that contains vertices a and b but not c, and a different cycle that contains b and c but not a, then it contains a cycle that contains a, b and c.

Problem 2. (10 points) We define the following predicates:

$F(x)$: x is Female; $S(x)$: x is a student; $K(x,y)$: x knows y's name.

Indicate which, if any, of the following expressions accurately translates the statement "Jill knows the name of every female student." There may be zero, or more than one correct answer.

[✓ i)] $\forall x\big(K(Jill,x) \rightarrow (F(x) \wedge S(x))\big)$ Correct

ii) $\neg\exists x\big(F(x) \wedge S(x) \wedge \neg K(Jill,x)\big)$

iii) $\forall x\big(\neg F(x) \vee \neg S(x) \vee K(Jill,x)\big)$

iv) $\forall x\big((F(x) \wedge S(x)) \rightarrow K(Jill,x)\big)$

[✓ v)] $\neg\exists x\big(F(x) \wedge S(x) \wedge K(Jill,x)\big)$ Correct

Problem 3. (15 points) Find a solution for x that satisfies the following system of congruences. First transform the congruences into the form used by the Chinese Remaindering method presented in lecture. Show your work in the bluebook. Fill in the table below.

$$3x \equiv 2 \pmod 5$$
$$3x \equiv 21 \pmod 7$$
$$7x \equiv 14 \pmod 8$$

$m =$ 280 ✓		
$a_1 =$ 2 ×	$m_1 =$ 56	$y_1 =$ 2 ×
$a_2 =$ 21 ×	$m_2 =$ 40	$y_2 =$ 7 ×
$a_3 =$ 14 ×	$m_3 =$ 35	$y_3 =$ 2 ×
$x \equiv$ 1114 $(mod\ m)$ = 274 ×		

Problem 4. (5 points) Evaluate each of the following, showing all steps of your work. You do not need a calculator for this problem.

a. Inverse of 8 (mod 29) ✓

b. $13^{493}\ (mod\ 7)$

c. $39^{89} (mod\ 13)$

Problem 5. (10 points) Define the sequence F_n of Fermat numbers as $F_n = 2^{2^n} + 1, n \geq 0.$

a) What are the values of F_0, F_1, F_2, F_3?

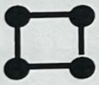
b) Prove by induction that $\forall n \geq 1$: $F_n = (F_0 \cdot F_1 \cdots F_{n-1}) + 2$

c) Prove that $\gcd(F_n, F_k) = 1$ for all $k < n$.
(Hint: use the result of part b, even if you have not proved it.) ✓

Problem 6. (10 points) Upon learning about graphs, Lem E. Hackett has, not unexpectedly, developed a proof for a claim that is clearly bogus. The claim relates to undirected graphs with no self-loops and no multiple edges connecting two vertices.

Claim: Every undirected graph $G(V, E)$ with three or more vertices, in which every vertex has degree two or more, contains a cycle of length three.

The claim is clearly false; the graph below does not contain a cycle of length 3.



What is the flaw in Lem's proof below.
Lem's Proof: By induction on the number of vertices in the graph.
Base Case: $|V| = 3$. In this case the only graph in which every vertex has degree two or more is the cycle of length 3. So, the claim is true in this case.
Inductive Hypothesis: For some $k \geq 3$ the claim is true for all graphs with k vertices.
Inductive Step: Let G be a graph with k vertices. By the inductive hypothesis it contains a cycle of length 3. Now add the $(k+1)^{st}$ vertex to G and connect it using two or more edges to two or more vertices in G. This gives a graph G' with $k+1$ vertices. Since G contained a cycle of length 3, adding a vertex and edges did not remove the cycle of length 3 which is contained in G'. This establishes the inductive step, and the claim is proved. ✓

3 edges!

Problem 7. (10 points) Prove by contradiction the following statement: If every vertex in an n-vertex graph has degree at least $\left\lceil \frac{n-1}{2} \right\rceil$ then the graph is connected. ($\lceil x \rceil$ denotes the smallest integer greater than or equal to x.)

✓

Problem 8. (10 points) Prove by contradiction the following statement: If 10 baseball batters hit a combined total of 30 home runs, then two or more batters hit the same number of home runs.

Problem 9. (10 points) When Lem walks upstairs, he can climb either one stair or two stairs in one step. For example, when he must climb 4 stairs, Lem can choose among the following 5 sequences:
1111 (one stair per step), or 112 (one stair in each of the first two steps, and two stairs in the third), or 121, 211, or 22.

a) How many different sequences can Lem choose from to climb 2 stairs?
b) How many different sequences can Lem choose from to climb 3 stairs?
c) How many different sequences can Lem choose from to climb 4 stairs?
d) How many different sequences can Lem choose from to climb 5 stairs?
e) Write a recurrence relation for S_n, the number of different sequences to climb $n \geq 1$ stairs. Explain your reasoning.

Extra Credit Problem. (10 points) Alice and Bob plan to use RSA public keys to exchange secret messages. Bob generates his keys using software written for him by ace programmer Lem E. Hackett.

Lem's software generates keys as follows:

1. $n = pq,$ where p, q are primes
2. e is chosen such that $\gcd\big(e, \phi(pq)\big) = 1$, where $\phi(pq) = (p-1)(q-1)$
3. The pair (n, e) is the public key.
4. Instead of generating d so that $de \equiv 1 \ \big(mod\ \phi(pq)\big)$, Lem's software has a bug (surprise!) and instead generates the private key d such that $de \ \equiv 1 \ \big(mod\ 4\phi(pq)\big)$.
5. Alice encrypts the plaintext m and sends Bob the ciphertext $c = m^e \ (mod\ n)$.
6. Lem tells Bob about the bug in generating the private key d. Bob is livid, but Lem assures Bob not to worry. After all, multiplying the modulus by 4 is just a left-shift by 2 bits which shouldn't make any difference in recovering Alice's plaintext.

Will Bob recover Alice's plaintext using Lem's buggy private key? Explain your answer.

Enjoy the summer break! Rest up, recharge, and see you in the Fall!