CS 70	Discrete Mathematics for CS	
Spring 2008	David Wagner	MT 1

PRINT your name: ______________________________, ______________________________
(last) (first)

SIGN your name: ____

PRINT your Unix account login: ____

Name of the person sitting to your left: ___________________________

Name of the person sitting to your right: ___________________________

You may consult any books, notes, or other paper-based inanimate objects available to you. Calculators and computers are not permitted. Please write your answers in the spaces provided in the test; in particular, we will not grade anything on the back of an exam page unless we are clearly told on the front of the page to look there.

You have 50 minutes. There are 3 questions, of varying credit (40 points total). The questions are of varying difficulty, so avoid spending too long on any one question.

Do not turn this page until your instructor tells you to do so.

Problem 1	
Problem 2	
Problem 3	
Total	

Problem 1. [True or false] (20 points)

Circle TRUE or FALSE. Do not justify your answers on this problem.

Reminder: $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ represents the set of non-negative integers and $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$ represents the set of all integers.

(a) TRUE or FALSE: Let the logical proposition $R(x)$ be given by $x^2 = 4 \implies x \leq 1$. Then $R(3)$ is true.

(b) TRUE or FALSE: The proposition $P \implies (P \wedge Q)$ is logically equivalent to $P \implies Q$.

(c) TRUE or FALSE: The proposition $P \implies (P \wedge Q)$ is logically equivalent to $(P \wedge Q) \implies P$.

(d) TRUE or FALSE: The proposition $(P \wedge Q) \vee (\neg P \vee \neg Q)$ is a tautology, i.e., is logically equivalent to True.

(e) TRUE or FALSE: $\exists n \in \mathbb{N} \,.\, (P(n) \wedge Q(n))$ is logically equivalent to $(\exists n \in \mathbb{N} \,.\, P(n)) \wedge (\exists n \in \mathbb{N} \,.\, Q(n))$.

(f) TRUE or FALSE: $\exists n \in \mathbb{N} \,.\, (P(n) \vee Q(n))$ is logically equivalent to $(\exists n \in \mathbb{N} \,.\, P(n)) \vee (\exists n \in \mathbb{N} \,.\, Q(n))$.

(g) TRUE or FALSE: $\forall n \in \mathbb{N} \,.\, ((\exists k \in \mathbb{N} \,.\, n = 2k) \vee (\exists k \in \mathbb{N} \,.\, n = 2k+1))$.

(h) TRUE or FALSE: $\exists n \in \mathbb{N} \,.\, ((\forall k \in \mathbb{N} \,.\, n = 2k) \vee (\forall k \in \mathbb{N} \,.\, n = 2k+1))$.

(i) TRUE or FALSE: $\forall n \in \mathbb{N} \,.\, ((\exists k \in \mathbb{N} \,.\, n = k^2) \implies (\exists \ell \in \mathbb{N} \,.\, n = \sum_{i=1}^{\ell} (2i-1)))$.

(j) TRUE or FALSE: If we want to prove the statement $x^2 \leq 1 \implies x \leq 1$ using Proof by Contrapositive, it suffices to prove the statement $x^2 > 1 \implies x > 1$.

(k) TRUE or FALSE: If we want to prove the statement $x^2 \leq 1 \implies x \leq 1$ using Proof by Contradiction, it suffices to start by assuming that $x^2 \leq 1 \wedge x > 1$ and then demonstrate that this leads to a contradiction.

(l) TRUE or FALSE: Let $S = \{x \in \mathbb{Z} : x^2 \equiv 2 \pmod 7\}$. Then the well ordering principle guarantees that S has a smallest element.

(m) TRUE or FALSE: Let $T = \{n \in \mathbb{N} : n^2 \equiv 2 \pmod 8\}$. Then the well ordering principle guarantees that T has a smallest element.

(n) Suppose that, on day k of some execution of the Traditional Marriage Algorithm, Alice likes the boy who she currently has on a string better than the boy who Betty has on a string.

TRUE or FALSE: It's guaranteed that on every subsequent day, this will continue to be true.

Problem 2. [You complete the proof] (10 points)

The algorithm $A(\cdot,\cdot)$ accepts two natural numbers as input, and is defined as follows:

$A(n,m)$:
1. If $n = 0$ or $m = 0$, return 0.
2. Otherwise, return $A(n-1,m) + A(n,m-1) + 1 - A(n-1,m-1)$.

Fill in the boxes below in a way that will make the entire proof valid.

Theorem: For every $n,m \in \mathbb{N}$, we have $A(n,m) = nm$.

Proof: If $s \in \mathbb{N}$, let $P(s)$ denote the proposition

"$\forall n,m \in \mathbb{N}\ .\ n+m = s \implies$ [ ]."

We will use a proof by [ ]

on the variable [ ].

Base case: $A(0,0) = 0$, so $P(0)$ is true.

Inductive hypothesis: Assume [ ]
is true for some $s \in \mathbb{N}$.

Induction step: Consider an arbitrary choice of $n,m \in \mathbb{N}$ such that $n+m = s+1$. If $n = 0$ or $m = 0$, then $A(n,m) = 0 = nm$ is trivially true, so assume that $n \geq 1$ and $m \geq 1$. In this case we see that

$$\begin{aligned} A(n,m) &= A(n-1,m) + A(n,m-1) + 1 - A(n-1,m-1) && \text{(by the definition of } A(n,m)\text{)} \\ &= (n-1)m + n(m-1) + 1 - (n-1)(m-1) && \text{(by the inductive hypothesis)} \\ &= nm - m + nm - n + 1 - nm + n + m - 1 \\ &= nm. \end{aligned}$$

In every case where $n+m = s+1$, we see that $A(n,m) = nm$. Therefore $P(s+1)$ follows from the inductive hypothesis, and so the theorem is true. □

Problem 3. [Modular arithmetic] (10 points)

Suppose that x, y are integers such that

$$3x + 2y = 0 \pmod{71}$$
$$2x + 2y = 1 \pmod{71}$$

Solve for x, y. Find all solutions. Show your work. Circle your final answer showing all solutions for x, y.