CS70, Fall 2006, Midterm 1, Papadimitriou & Vazirani

1. (*50 points*) Short Answer Grab Bag

True or False

T F If a has an inverse modulo b, then b has an inverse modulo a.

T F If $ax \equiv bx \bmod c$, then $a \equiv b \bmod c$

T F The propose and reject algorithm for stable marriage always lasts for at least two days.

T F It is possible that man M is paired with woman W in both a man optimal pairing and a woman optimal pairing.

T F The converse of the statement "if n is odd then so is n^4", is "if n is not odd then n^4 is not odd".

T F In a proof by contraposition of the statement "if n is odd then so is n^4", you would assume that n is not odd.

T F In a proof by contradiction of the statement "if n is odd then so is n^4", you would assume that n is odd and n^4 is even.

T F There are 49 polynomials P(x) of degree (at most) 3 over the field GF_7 such that P(5) = 6.

T F In an [n,2] secret sharing scheme (i.e. any two players can reconstruct the secret) modulo 19, player 1 and player 6 together try to reconstruct the secret. Suppose player 1's share is 2 and player 6's share is 9, then the secret must be 12.

T F There are at least two distinct polynomials of degree 5 over GF_{19} that have the same values at 5 distinct points.

For the following parts assume that P(n) and Q(n) are predicates on the natural numbers, and suppose:

$$\forall k \in N, P(k) \Rightarrow Q(k+1), and \forall k \in N, Q(k) \Rightarrow P(k+1)$$

For each of the following assertions below, circle the correct alternative: (A) it must always hold, or (N) it can never hold, or (C) it can hold but need not always.
The domain of all quantifiers is the natural numbers.

A N C $(P(0) \vee Q(0)) \Rightarrow \forall n P(n)$

A N C $(P(0) \wedge Q(0)) \Rightarrow \forall n P(n)$

A N C $(P(0) \wedge Q(0)) \Rightarrow \forall n (P(n) \wedge Q(n))$

A N C $(P(0) \vee Q(0)) \Rightarrow \forall n (P(n) \vee Q(n))$

A N C $(\neg P(201) \wedge \neg Q(201)) \Rightarrow (\neg P(0) \vee \neg Q(0))$

2. (*30 points*) Induction

Prove by induction that for every odd number n, $3^n + 4^n$ is divisible by 7.

State formally the statement you are proving by induction:

Proof by induction on:

Base Case:

Induction Hypothesis:

Induction Step:

CS70, Fall 2006, Midterm 1, Papadimitriou & Vazirani

3. (*20 points*) Modular Arithmetic

Solve for x and y:
$3x + 5y = 2 \bmod 19$
$7x + 3y = 8 \bmod 19$