CSE 321 Winter 2007 Midterm

1. (15 points)

   (a) Use the extended Euclidean algorithm to solve $33x \equiv 4 \pmod{7}$ fox x.

   (b) Find an inverse of 7 modulo 33.

2. (15 points) Let n be an integer. Prove that if nx is irrational, then x is irrational.

3. (15 points) Circle T or F to indicate whether each of the following statements is true or false. If the answer is false, *briefly* explain why. Assume positive integers for all numbers.

   (a) If $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$. .... T F

   (b) If $a|c$, then $\exists b(a|b \wedge b|c)$. .... T F

   (c) $\gcd(a, a \bmod b) \leq \gcd(a, b)$. .... T F

   (d) If $\gcd(a, b) = \gcd(b, c)$, then $\gcd(a, b) = \gcd(a, c)$. .... T F

   (e) $(\neg p \wedge \neg q) \rightarrow \neg(p \vee q)$ is a tautology. .... T F

   (f) $q \rightarrow (p \vee \neg p)$ is a tautology. .... T F

   (g) $(p \rightarrow q) \rightarrow (q \rightarrow p)$ is a tautology. .... T F

4. (15 points) Define the following predicates.

   - $M(x, y)$: "x is married to y"
   - $S(x, y)$: "x is a sibling of y"
   - $F(x)$: "x is female"
   - $P(x, y)$: "x is a (biological) parent of y"

   Let the universe for all variables be the set of all people. Do *not* use the uniqueness quantifier, $\exists!$. Express the following:

   (a) Everyone is married to at most one person.

   (b) Tom is an only child (i.e. has no siblings).

   (c) Siblings have a common (biological) parent.

   (d) Alice is Bob's half-sister. (Alice and Bob have exactly one common biological parent.)

5. (20 points) Prove that for every positive integer n, $\sum_{k=1}^{n} k2^k = (n-1)2^{n+1} + 2$.

6. (10 points) What is $16^{15} \bmod 7$?

7. (10 points) Find the flaw with the following "proof" that $a^n = 1$ for all nonnegative integers n, whenever a is a nonzero real number.

   Basis Step: $a^0 = 1$ is true by the definition of a^0.

   Inductive Step: Assume that $a^j = 1$ for all nonnegative integers j with $j \leq k$. Then note that

$$a^{k+1} = \frac{a^k \cdot a^k}{a^{k-1}} = \frac{1 \cdot 1}{1} = 1.$$

   Try not to use more than 50 words.

Equivalences	
Identity Laws	$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$
Domination Laws	$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$
Idempotent Laws	$p \vee p \equiv p$ $p \wedge p \equiv p$
Commutative Laws	$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$
Associative Laws	$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
Distributive Laws	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
De Morgan's Laws	$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$
Negation Laws	$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$
Double Negation Law	$\neg\neg p \equiv p$
Contrapositive Law	$p \rightarrow q \equiv \neg q \rightarrow \neg p$
Implication Law	$p \rightarrow q \equiv \neg p \vee q$
Quantifier Negation Laws	$\neg \exists x P(x) \equiv \forall x \neg P(x)$ $\neg \forall x P(x) \equiv \exists x \neg P(x)$

Propositional and Predicate Equivalences

Inferences	
Modus Ponens	$\dfrac{p,\ p \to q}{\therefore q}$
Direct Proof	$\dfrac{p \Rightarrow q}{\therefore p \to q}$
Simplification	$\dfrac{p \wedge q}{\therefore p,\ q}$
Consolidation	$\dfrac{p,\ q}{\therefore p \wedge q}$
Disjunctive Syllogism	$\dfrac{p \vee q,\ \neg p}{\therefore q}$
Addition	$\dfrac{p}{\therefore p \vee q,\ q \vee p}$
Excluded Middle	$\dfrac{}{\therefore p \vee \neg p}$
Universal Instantiation	$\dfrac{\forall x P(x)}{\therefore P(c):\ c \text{ arbitrary}}$
Universal Generalization	$\dfrac{P(c):\ c \text{ arbitrary; no dependency}}{\therefore \forall x P(x)}$
Existential Instantiation	$\dfrac{\exists x P(x)}{\therefore P(c):\ c \text{ new and specific; depends on ...}}$
Existential Generalization	$\dfrac{P(c):\ c \text{ specific or arbitrary}}{\therefore \exists x P(x)}$

Propositional and Predicate Inferences