Fall 2015
Midterm review session

Test:
1. When did the Pilgrims land at Plymouth Rock?

1620.

As you can see, I've memorized this utterly useless fact long enough to pass a test question. I now intend to forget it forever. You've taught me nothing except how to cynically manipulate the system. Congratulations.

They say the satisfaction of teaching makes up for the lousy pay.
The domain of discourse is the set of all people in Washington and the set of all paper-based objects.

The predicates are $\text{Student}(x)$, $\text{Exam}(x)$, $\text{Takes}(x, y)$ (meaning that student $x$ takes exam $y$), and $\text{Equal}(x, y)$ (meaning that $x$ and $y$ are the same object).

“All exams are taken by at least one student.”

\[
\forall x \left( \text{Exam}(x) \implies \exists y \left( \text{Student}(y) \land \text{Takes}(y, x) \right) \right)
\]

“Every student takes exactly one exam.”

\[
\forall x \left( \text{Student}(x) \implies \left( \forall y \forall z \left( \text{Exam}(y) \land \text{Exam}(z) \land \text{Takes}(y, x) \land \text{Takes}(z, x) \land \neg \text{Equal}(y, z) \right) \right) \right)
\]
The domain of discourse is the set of all people in Washington and the set of all paper-based objects.

The predicates are \( \text{Student}(x), \text{Exam}(x), \text{Takes}(x, y) \) (meaning that student \( x \) takes exam \( y \)), and \( \text{Equal}(x, y) \) (meaning that \( x \) and \( y \) are the same object).

Translate the following statement into English (try to make the translation as simple as possible):

\[
\forall x \forall y \ ((\text{Student}(x) \land \text{Student}(y) \land \neg \text{Equal}(x, y)) \rightarrow (\exists z \ \text{Exam}(z) \land \text{Takes}(x, z) \land \neg \text{Takes}(y, z)))
\]

For all pairs of distinct students, there is an exam that one student takes, but the other student doesn't.
Design a circuit with **three inputs** that computes the function $M(p, q, r)$ where

\[
M(T, q, r) = q \land r \\
M(F, q, r) = q \lor r
\]

\[
M = pqr + p'qr + p'q'r + p'q'r' \]

\[
M = q'r + p'(q'r + qr')
\]
Each of the following functions maps the non-negative integers \( \mathbb{N} \) to the non-negative integers \( \mathbb{N} \). For each one, indicate the following: (i) whether the function is one-to-one, (ii) whether the function is onto. Briefly justify your answers.

(a) \( f(n) = 3^n \)  
   \[ f(n) \text{ is never even} \]
   \[ f(n) \text{ is never one-to-one} \]

(b) \( f(n) = n + 1 \) if \( n \) is even and \( f(n) = 3n + 1 \) if \( n \) is odd.  
   \[ \text{both cases are increasing} \]
   \[ \text{1st case outputs odd, 2nd case outputs even} \]

(c) \( f(n) = n^2 - 2n + 1 \)  

(d) \( f(n) = \) the smallest integer \( k \) such that \( 3^k \geq n + 1 \).

(e) \( f(n) = \) # of distinct prime factors dividing \( n + 1 \).  
   \[ f(2) = f(4) = 1 \]  
   \[ f(0) = 0 \]  
   and \( f(p_1 \cdots p_k) = k \)
Prove that \( A = B \) if and only if \( \mathcal{P}(\mathcal{P}(A)) = \mathcal{P}(\mathcal{P}(B)) \).

(Tricky)

Just prove \[ A = B \iff \mathcal{P}(A) = \mathcal{P}(B) \]
\( \iff \mathcal{P}(\mathcal{P}(A)) = \mathcal{P}(\mathcal{P}(B)) \)

\[ \begin{align*}
A = B & \iff \forall x (x \in A \iff x \in B) \\
& \iff \forall x (x \in \mathcal{P}(A) \iff x \subseteq A) \\
& \iff \forall x (x \in \mathcal{P}(A) \iff x \subseteq B) \\
& \iff \forall x (x \in \mathcal{P}(\mathcal{P}(A)) \iff x \subseteq \mathcal{P}(B))
\end{align*} \]

Suppose \( A = B \). Then \( \forall x \)
\[ x \in \mathcal{P}(A) \iff x \subseteq A \iff x \subseteq B \iff x \in \mathcal{P}(B) \]

Hence \( \mathcal{P}(A) = \mathcal{P}(B) \).

Suppose \( \mathcal{P}(A) = \mathcal{P}(B) \). Then \( \forall x \)
\[ x \in A \iff \{x\} \subseteq A \iff \{x\} \in \mathcal{P}(A) \]
\[ \implies A = B. \]
Prove that for every positive integer $n$, it holds that

$$P(n) = \sum_{k=1}^{n} k \cdot 2^k = (n-1)2^{n+1} + 2$$

**Base case:** $P(1) = 1 \cdot 2^1 = (1-1)2^{1+1} + 2$

$$2 = 2 \quad \text{true}$$

**IH:** Assume $P(j)$ for some $j \geq 1$

**IS:** By the IH, $\sum_{k=1}^{j} k \cdot 2^k = (j-1)2^{j+1} + 2$

Add $(j+1)2^{j+1}$ to both sides:

$$\sum_{k=1}^{j+1} k \cdot 2^k = (j-1)2^{j+1} + 2 + (j+1)2^{j+1}$$

Therefore by induction, $P(n)$ holds for all $n \geq 1$. 
Prove that if $n > 6$ is an integer then $3^n < n!$
Prove that if $p$ is a prime number and $ab \equiv ac \pmod{p}$ then either
\[ a \equiv 0 \pmod{p} \quad \text{or} \quad b \equiv c \pmod{p} \]

(1) \hspace{1cm} ab \equiv ac \pmod{p} \Rightarrow a(b-c) \equiv 0 \pmod{p} \\
\Rightarrow p \mid a(b-c) \\
\Rightarrow p \mid a \quad \text{or} \quad p \mid b-c \quad \text{by unique factorization} \\
\Rightarrow a \equiv 0 \pmod{p} \quad \text{or} \quad b \equiv c \pmod{p} \\
\text{If } a \equiv 0 \pmod{p} \text{ then } \smiley

(2) \hspace{1cm} \text{If } a \not\equiv 0 \pmod{p} \text{ then } \gcd(a, p) = 1 \\
b/c \text{ p is prime } \Rightarrow \exists \text{ multiplicative inverse } a^{-1} \pmod{p} \\
\text{So } a^{-1}(ab) \equiv a^{-1}(ac) \pmod{p} \\
\Rightarrow b \equiv c \pmod{p}.
Give a formal proof that:

\( \forall x \ (P(x) \land \forall x \ Q(x)) \rightarrow \forall x \ (P(x) \rightarrow Q(x)) \)

By direct proof:

1) \( \forall x \ P(x) \land \forall x \ Q(x) \)

2) \( \forall x \ P(x) \)

3) \( \forall x \ Q(x) \)

4) \( P(c) \) for some \( c \)

5) \( Q(c) \)

6) \( \neg \neg P(c) \)

7) \( P(c) \rightarrow Q(c) \)

8) \( \forall x \ (P(x) \rightarrow Q(x)) \) \( \triangleright \) \( c \) arbitrary \( \blacksquare \)
Some red cats don’t like tofu.

\[ \exists x \,(\text{Red}(x) \land \text{Cat}(x) \land \neg \text{LikesTofu}(x)) \]

Incorrect:

\[ \exists x \,(\text{Red}(x) \land \text{Cat}(x) \rightarrow \neg \text{LikesTofu}) \]