CS 70 Discrete Mathematics and Probability Theory
Fall 2012 Vazirani Midterm 1

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

PRINT your GSI name and discussion section: _____

Name of the person sitting to your left: _____

Name of the person sitting to your right: _____

You may consult one single-sided sheet of notes. Calculators are not permitted, and cellphones must be turned off and put away. Do all your work on the pages of this examination. Give reasons for all your answers. Good Luck!

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.

(a) $(P \Rightarrow Q) \Rightarrow (\neg Q \Rightarrow \neg P)$

(b) $(P \wedge Q) \Rightarrow (P \Rightarrow Q)$

(c) $(P \Rightarrow (P \wedge Q)) \Rightarrow (P \Rightarrow Q)$

(d) $\neg(\forall x \in \mathbf{N} \ \ \exists y \in \mathbf{N} \ \ P(x,y)) \ \Rightarrow \ (\exists x \in \mathbf{N} \ \ \forall y \in \mathbf{N} \ \ \neg P(x,y))$

(e) $\forall x \in \mathbf{N} \ \ \exists y \in \mathbf{N} \ \ \forall z \in \mathbf{N} \ \ x - y \leq z$

(f) $\forall x \in \mathbf{Z} \ \ \exists y \in \mathbf{Z} \ \ \forall z \in \mathbf{Z} \ \ x - y \leq z$

(g) $\forall x, y \in \mathbf{N} \ \ gcd(2x, 2y) = 2gcd(x, y)$

(h) $\forall x, y \in \mathbf{N} \quad gcd(2x, 4y) = 2gcd(x, y)$

(i) For all $x, y \in \mathbf{N}$, if $6x \equiv y \pmod{11}$, then $x \equiv 6y \pmod{11}$.

(j) In every stable pairing that is pessimal for a woman, that woman is matched to her least favorite man.

2. Modular Arithmetic (40 points)

(a) Let p be prime. Simplify $1^p + 2^p + \cdots + p^p \pmod{p}$.

(b) Compute $8^{-1} (\text{mod} 21)$ using Euclid's extended GCD algorithm. Show your steps.

(c) Bijections & RSA: For each of the following functions f on the numbers modulo 35 (i.e. $f : S \to S$, where $S = \{0, 1, \ldots, 34\}$) indicate whether f is a bijection or not by circling the appropriate choice.

- $f(x) = 3x \pmod{35}$
- $f(x) = 5x \pmod{35}$
- $f(x) = x - 6 \pmod{35}$
- $f(x) = x/8 \pmod{35}$
- $f(x) = x^{25} \pmod{35}$
- $f(x) = x^5 \pmod{35}$
- $f(x) = x^2 \pmod{35}$
- $f(x) = x^{10} \pmod{35}$

3. Proofs (30 points)

(a) Grade these attempts at executing the stated proof strategies Pass or Fail, with one or two lines of justification:

- You wish to prove by contradiction that $x < y$ implies $x^2 < y^2$.
  So you start by assuming for contradiction that $x \geq y$ and $x^2 \geq y^2$.

- You wish to prove by contradiction that $x < y$ implies $x^2 < y^2$.
  So you start by assuming for contradiction that $x \geq y$ and $x^2 < y^2$.

- You wish to prove by contraposition that $\exists x\ P(x) \Rightarrow \forall x\ Q(x)$.
  So you start by assuming $\exists x\ \neg Q(x)$.

- You wish to prove by contraposition that $\exists x\ P(x) \Rightarrow \forall x\ Q(x)$.
  So you start by assuming $\forall x\ Q(x)$.

(b) You wish to break a standard $m \times n$ Hershey chocolate bar into mn little squares to distribute to mn kids. In each step you can pick up exactly one piece of chocolate and break it along one of the horizontal or vertical lines etched into the bar. No stacking! Prove by induction that the minimum number of steps required to completely break the bar into mn little squares is $mn - 1$.

Proof by induction on:

Base Case:

Induction Hypothesis:

Induction Step: