CS 70	Discrete Mathematics and Probability Theory	
Fall 2011	Rao	Midterm 1

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

SIGN your name: ____

PRINT your discussion section number (101–108): ____

Name of the person sitting to your left: ___________________________

Name of the person sitting to your right: ___________________________

You may consult a single, double-sided sheet of paper with notes. Apart from that, you may not look at books, notes, etc. Calculators and computers are not permitted. Please write your answers in the spaces provided in the test. 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 120 minutes. There are 4 questions, of varying credit (100 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	
Problem 4	
Total	

Problem 1. Quantifiers [8 points]

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

Let $P(k)$ be a proposition involving a natural number k. Suppose you know only that $(\forall k \in \mathbb{N})(P(k) \Rightarrow P(2k))$. For each of the propositions below, state T if it is definitely true, F it is definitely false, or D if it could be true or false depending on P.

(a) $(\forall n \in \mathbb{N})(P(n))$.

(b) $(P(0) \wedge P(1)) \Rightarrow ((\forall n \in \mathbb{N})(P(n)))$

(c) $((\forall n \in \mathbb{N})(n \text{ is odd } \Rightarrow P(n))) \Rightarrow ((\forall n \in \mathbb{N})(n \geq 1 \Rightarrow P(n)))$

(d) $(\forall n \in \mathbb{N})(P(2n))$.

Problem 2. [True or false] (13 points)

Circle TRUE or FALSE. Do not justify your answers on this problem.
(Don't write anything. Just circle the right answer.)

(a) TRUE or FALSE: $(\forall n \in \mathbb{N})\neg(n > 3 \wedge n^2 < 16)$

(b) TRUE or FALSE: $(P \implies Q) \vee (Q \implies P)$

(c) TRUE or FALSE: $(P \wedge Q) \vee R \equiv (P \wedge R) \vee (Q \wedge R)$

(d) TRUE or FALSE: For all $x, y \in \mathbb{N}$, if $x + 7 \equiv y + 7 \pmod 9$, then $x \equiv y - 7 \pmod 9$.

(e) TRUE or FALSE: For all $x, y \in \mathbb{N}$, if $4x \equiv y \pmod 9$, then $x \equiv 7y \pmod 9$.

(f) TRUE or FALSE: $\gcd(453, 368) = \gcd(85, 368)$.

(g) TRUE or FALSE: For all $x, d, m \in \mathbb{N}$, $\gcd(x, m) = d > 1$, then there exist $k \in \{1, \ldots, m-1\}$ where $kx \equiv 0 \pmod m$

(h) TRUE or FALSE: For all $x \in \mathbb{N}$ and prime p then there exist $k \in \{1, \ldots, p-1\}$ where $kx \equiv 0 \pmod p$

(i) TRUE or FALSE: The product $P(x) \cdot Q(x)$ of two degree ≤ 5 nontrivial (not constantly equal to zero) polynomials $P(x)$ and $Q(x)$ can only be zero at 5 x-values.

(j) TRUE or FALSE: Given 8 points, there are two different degree ≤ 3 polynomials that contain at least 5 of the 8 points. (The different polynomials may pass through a different subset of 5 points.)

(k) TRUE or FALSE: Given 8 points, there are at least two different degree ≤ 3 polynomials that contain 6 of the 8 points.

(l) TRUE or FALSE: Given 8 points, there can be two different degree ≤ 3 polynomials that contain 7 of the 8 points.

(m) TRUE or FALSE: In every stable pairing that is pessimal for a woman, that woman is matched to her least favorite man.

3. How many? What expression? (54 points)

Full credit for correct answers. There is a some chance we will give partial credit for small errors, so you may wish to provide an concise explanation. **But don't waste time on long explanations!**

(a) A dudoko grid consists of an 2×4 grid filled with the numbers $1, \ldots, 4$. Moreover, each row contains all 4 numbers, the leftmost 2×2 subgrid contains all 4 numbers and the rightmost 2×2 subgrid contains all 4 numbers. For example,

1	2	3	4
3	4	1	2

How many different 2×4 dudoku configurations?

(b) How many rolls of 6 dice with exactly 5 distinct values (the dice are distinguishable)?

(c) How many diagonals are there for a convex n vertex polygon? (A diagonal is a line segment between two nonadjacent vertices.)

(d) How many increasing sequences of k numbers from $\{1, \ldots, n\}$? ($2, 3, 5, 5, 7$ is not an increasing sequence.)

(e) How many nondecreasing sequences of k numbers from $\{1, \ldots, n\}$? ($2, 3, 5, 5, 7$ is a nondecreasing sequence.)

(f) How many distinct degree $\leq d$ polynomials modulo p, where $d \leq p - 1$?

(g) How many distinct degree $\leq d$ polynomials with exactly d roots modulo p where $d \leq p - 1$? (Brief explanation ok.)

(h) A message is encoded using a degree ≤ 2 polynomial, $P(x)$, modulo 5. What is the coefficient of x^2 when the polynomial contains the points $(1, 2), (2, 1), (3, 0)$ (each point is in the form $(x, P(x))$)?

(i) How many values of $x \in \{0,\dots,11\}$ satisfy $4x = 6 \pmod{12}$?

(j) How many values of $x \in \{0,\dots,11\}$ satisfy $8x = 4 \pmod{12}$?

(k) How many values of x in $\{0,\dots,m-1\}$ satisfy $nx = b \pmod{m}$ when $d = gcd(m,n) > 1$ and $gcd(n,b) < d$? State your answer as a function of n, m and d. (A function of n, m and d may only depend on a (possibly empty) subset of these variables.)

(l) How many values of $x \in \{0,\dots,m-1\}$ satisfy $nx = b \pmod{m}$ when $d = gcd(m,n) > 1$ and $d|b$? State your answer as a function of n, m and d.

(m) What is $15^{404} \pmod{37}$? (37 is prime.)

(n) What is $(9^5)^5 \pmod{35}$? (35 is not prime.)

(o) What is $1^p + 2^p + \dots (p-1)^p \pmod{p}$ where p is an odd prime?

(p) What is the last day Jung Lin could first be proposed to in any run of the TMA on n men and n women given that she is second on every man's preference list? As a function of n if necessary.

(q) What is the last day Sheila could first be proposed to in any run of the TMA that on n men and n women given that she is third on every man's preference list? As a function of n if necessary.

(r) What is the last day any woman is proposed to in a run of the TMA algorithm that is T days long?

Problem 4. Reviewing Simple Proofs. (25 points)

(a) Prove that $\sqrt{3}$ is irrational.

(You may use the fact that for a prime p: $p|n^2 \implies p|n$ for all natural numbers n.)

(b) Prove $3^{n+1} | 2^{3^n} + 1$ or give a counterexample.