Midterm 1

Friday, July 19, 5:10pm–7:10pm

CS 70: Discrete Mathematics and Probability Theory, Summer 2013

Your name ____________________________

Your student ID # ____________________________

Your section # ____________________________

This exam has 5 questions and a total of 100 points.
Do not open the exam until you are told to.
Do not write below this line.

Q1	
Q2	
Q3	
Q4	
Q5	
Total	

1. [30 points] **MULTIPLE CHOICE.** Circle the correct answer. You don't need to show work.

1a. [2 points] $\big(P \Rightarrow \neg(Q \wedge P)\big) \quad \equiv \quad (\neg P \vee Q)$

TRUE FALSE

1b. [2 points] $(\neg P \Rightarrow Q) \quad \equiv \quad (\neg Q \Rightarrow P)$

TRUE FALSE

1c. [2 points] If an implication is true, then its converse must be false.

TRUE FALSE

1d. [2 points] Is the following proposition true or false? $(\forall x \in \mathbb{N})\big((x^3 = x) \vee \neg(x^2 < 2x)\big)$

TRUE FALSE

1e. [2 points] Consider the proposition $\forall x\ \big((\exists y\ P(x,y)) \Rightarrow Q(x)\big)$. One of the following three propositions is logically equivalent to it. Which one?

$$\forall x\ \big((\exists y\ P(x,y)) \vee \neg Q(x)\big)$$

$$\neg\exists x\ \big((\forall y\ \neg P(x,y)) \vee Q(x)\big)$$

$$\neg\exists x\ \big((\exists y\ P(x,y)) \wedge \neg Q(x)\big)$$

1f. [2 points] Let $M(x)$ represent "x owns mittens" and $G(x)$ represent "x owns gloves". Which one of the following correctly expresses "Nobody owns both mittens and gloves"?

$$\forall x\ \big(G(x) \Rightarrow M(x)\big)$$

$$\forall x\ \big(G(x) \Rightarrow \neg M(x)\big)$$

$$\forall x\ \big(M(x) \Rightarrow G(x)\big)$$

$$\forall x\ \big(\neg M(x) \Rightarrow G(x)\big)$$

1g. [2 points] Suppose you want to prove a proposition $P \Rightarrow Q$. Which one of the following is *not* a valid proof strategy?

Assume $\neg Q$ and prove $\neg P$

For some R, assume $R \wedge P$ and prove Q, and then assume $(\neg R) \wedge P$ and prove Q

Assume $(P \Rightarrow Q)$ and prove $(R \wedge \neg R)$ for some R

1h. [2 points] Suppose you want to prove a proposition $(\forall x \in \mathbb{N})\ (P(x) \vee Q(x))$. Which one of the following three things is *not* a valid proof strategy?

For every $x \in \mathbb{N}$, assume $\neg Q(x)$ and prove $P(x)$

Prove $P(0)$, and for every $x \geq 1$, assume $(\forall y \in \mathbb{N})\ \big((y \leq x) \;\Rightarrow\; (P(y) \vee Q(y))\big)$ and prove $P(x+1) \vee Q(x+1)$

Prove $P(0)$, and for every $x \geq 1$, assume $\big(P(x-1) \vee Q(x-1)\big) \wedge \neg P(x) \wedge \neg Q(x)$ and prove $R \wedge \neg R$ for some R

1i. [2 points] In a stable marriage instance, if (M_1, W_1), (M_1, W_2), and (M_2, W_2) are all rogue couples with respect to some pairing, then (M_2, W_1) cannot be a rogue couple with respect to that pairing.

TRUE FALSE

1j. [2 points] In a stable marriage instance, if all the women have different favorite men, then the female-optimal algorithm will find the same stable pairing regardless of the men's preferences.

TRUE FALSE

1k. [2 points] For all positive integers $x > y$, $GCD(x, x-y) = GCD(y, x-y)$.

TRUE FALSE

1l. [2 points] If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ and $GCD(c, m) = GCD(d, m) = 1$, then $(a/c) \equiv (b/d) \pmod{m}$, where the division is "mod m" division.

TRUE FALSE

1m. [2 points] Which one of the following does Fermat's Little Theorem apply directly to?

26^{12} mod 13 7^{14} mod 15 22^{16} mod 17 9^{11} mod 19

1n. [2 points] Suppose you run the secret-sharing scheme over $GF(17)$ by letting your secret be the constant coefficient of a degree-4 polynomial. If two people decide to collude, how many more people must they convince to join before they can recover the secret?

1 2 3 4 5

1o. [2 points] Alice has a message of 4 packets over $GF(7)$ that she would like to communicate to Bob. She uses the polynomial error-correction scheme and sends 5 packets across the network to Bob. Three of these packets get dropped. From Bob's point of view, how many possibilities are there for Alice's original message? (Bob knows that the original message was 4 packets long.)

1 7 8 49 50

2. [16 points] **INDUCTION.**

   Let's revisit the party from Section 2. Recall that a *celebrity* is a guest who is known by all other guests, but knows none of them. Prove that if the following both hold:

   (i) for every pair of guests A and B, either A knows B, or B knows A, but not both, and

   (ii) there do not exist guests A, B, C such that A knows B, B knows C, and C knows A,

   then the party has a celebrity. Your proof must use induction on n (the number of guests at the party) to receive credit. Clearly label all parts of your proof, and include all details.

3. [16 points] **STABLE MARRIAGE.**

Consider the following stable marriage instance.

Man	Women			
1	A	C	B	D
2	B	C	D	A
3	B	A	C	D
4	B	A	D	C

Woman	Men			
A	2	4	1	3
B	3	1	4	2
C	1	4	2	3
D	3	4	2	1

3a. [6 points] List all the rogue couples for the following pairing: (1,A), (2,B), (3,C), (4,D)

3b. [10 points] For each man, find his optimal woman and his pessimal woman. Show all your work and justify your answer.

4. [20 points] **MODULAR ARITHMETIC.**

4a. [5 points] Use the Extended Euclidean Algorithm to compute $GCD(54, 21)$ and express it as $a \cdot 54 + b \cdot 21$. Show your work.

4b. [5 points] Solve for (the congruence class of) x in the following equation:

$$x^{21} \equiv 4 \pmod{23}$$

(Hint: Find a way to make use of Fermat's Little Theorem.)

4c. [5 points] Compute $3^{10} \bmod 15$ using repeated squaring. Show your work.

4d. [5 points] Bob uses RSA and announces that his public key is $(N = 55, e = 27)$. Alice sends the ciphertext 4 to Bob. You are Eve, and you realize Bob was very foolish to use such a small value of N. Decrypt the ciphertext, and show your work.

5. [18 points] **POLYNOMIALS.**

5a. [10 points] A polynomial $q(x)$ over $GF(7)$ has the (point,value) representation

$$(1,1) \quad (2,0) \quad (3,2)$$

Find the following (point,value) representation of the same polynomial:

$$(0,q(0)) \quad (3,q(3)) \quad (4,q(4))$$

You should do this by first converting to the coefficient representation. Use methods that were taught in class, and show all intermediate steps. Clearly label your final answer.

5b. [3 points] In class we proved that any two distinct polynomials of degree $\leq d$ over $GF(p)$ can agree on at most d points. What is the smallest positive integer ℓ such that any ℓ distinct polynomials of degree $\leq d$ over $GF(p)$ can agree on at most $d-1$ points? (Note: Your answer for ℓ should be in terms of d and/or p.)

5c. [5 points] Prove the following theorem showing that your choice of ℓ from part (5b) works. (You do not need to prove that no smaller choice of ℓ satisfies the theorem.) You may use any result from class in your proof of the theorem.

> **Theorem:** For any ℓ distinct polynomials $q_1, q_2, \ldots, q_\ell$ of degree $\leq d$ over $GF(p)$, there are at most $d-1$ points x such that $q_1(x) = q_2(x) = \cdots = q_\ell(x)$.

Proof: