CS 70 First Midterm 10 July 2012

NAME (1 pt): _____

SID (1 pt): _____

TA (1 pt): _____

Name of Neighbor to your left (1 pt): _____

Name of Neighbor to your right (1 pt): _____

Instructions: This is a closed book, closed calculator, closed computer, closed network, open brain exam, but you are permitted a 1 page, double-sided set of notes, large enough to read without a magnifying glass.

You get one point each for filling in the 5 lines at the top of this page.

Write all your answers on this exam. If you need scratch paper, ask for it, write your name on each sheet, and attach it when you turn it in (we have a stapler).

1	
2	
3	
4	
5	
6	
Total	

1

Question 1 (20 points) Potpourri.

1.1 (14 points). True or False

For each of the following propositions, circle either T if it is always true, F if it is always false. You do not have to justify your answer. We let $\mathbb{N} = \{0, 1, 2, ...\}$ denote the non-negative integers, $\mathbb{Z}+ = \{1, 2, 3, ...\}$ denote the positive integers.

T F $(p \wedge \neg q) \wedge (\neg p \vee q) \wedge r$

T F $\forall x, y \in \mathbb{N}, z \in \mathbb{Z} + .[2x \equiv 2y \ (mod\ z) \implies x \equiv y \ (mod\ z)]$.

T F Given d pairs $(x_1, y_1), ..., (x_d, y_d)$, with all the x_i distinct, there is a unique polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for $1 \leq i \leq d$

T F $(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(x^6 = y^2)$

T F In a stable marriage instance, if a man and women have each other last on their respective lists, they are guaranteed not to be paired in any stable pairing.

T F $\forall x, y \in \mathbb{N}$, if $9x \equiv y \pmod{26}$, then $x \equiv 3y \pmod{26}$.

T F $\forall x, y \in \mathbb{N}$, $\gcd(2x, 3y) = \gcd(x, y)$.

1.2 (6 points). Prove or disprove the following proposition:

If every even number greater than 2 is the sum of 2 prime numbers, then every odd numbers greater than 7 is the sum of 3 prime numbers.

Question 2 (20 points) Induction: Poor Valentine.
A school teacher is preparing for Valentine's Day. She has instructed each student to make a Valentine. Then, to ensure fairness, she will have the everyone play the following game:
The students all wander randomly around the room for ten minutes, then gives his or her Valentine to the student closest to them. To further ensure fairness, the teacher adds the following rule: each student must keep every other student a different distance away from them.

Show that if the teacher has an odd number of students, one of them will not receive a Valentine. You may assume the class has more than one student.

2.1 (3 points). State and prove the base case for the induction.

2.2 (3 points). State the induction hypothesis.

2.3 (14 points). Complete the proof by stating and proving the induction step.

Question 3 (20 points) Stable Marriage.
For each of the following questions,

i) Fill in the tables with an example preference list, give a stable pairing for $n = 3$, and show that your example is correct.

ii) Generalize your example to an arbitrary n and show that your generalization is correct. You do not need to provide the stable pairing for your generalization.

3.1 (10 points). Consider a stable marriage instance where *Traditional Propose & Reject Algorithm* returns a pairing which is optimal for both male and female AND terminates after exactly 1 day.

3.2 (10 points). Consider a stable marriage instance where *Traditional Propose & Reject Algorithm* returns a "female optimal" pairing AND terminates after exactly n days.

Question 4 (15 points) Modular Arithmetic.

4.1 (10 points). Use the extended gcd algorithm to find $\gcd(47, 20)$ and find the numbers x and y where $47 * x + 20 * y = \gcd(47, 20)$

4.2 (5 points). Find a value for x that solves $47x \equiv 8 \pmod{20}$. Show your work.

Question 5 (15 points) RSA.

5.1 (5 points). Alice wants to send Bob a message $m = 5$ using his public key ($n = 26, e = 11$). What cipher text $E(m)$ will Alice send?

5.2 (10 points). Is Two Always Better than One?

One day, Joe Hacker decides that he wants to improve the security of RSA. He uses $N = pq$ as usual, but has each person send a message with a *different* exponent, e.

Suppose Alice and Bob each send the same message encrypted with their respective public keys, (N,e_1) and (N,e_2), and that Eve intercepts both encrypted messages, $c_1 = m^{e_1} \pmod N$ and $c_2 = m^{e_2} \pmod N$.

Show how Eve can use c_1, c_2, and both public keys to recover the original message m if e_1 and e_2 are relatively prime. (*Hint:* Consider using egcd)

Question 6 (20 points) Error Correcting Codes.

6.1 (5 points). Evaluate $f(x) = 3x^2 - x + 1$ on every point of *GF(5)*.

6.2 (5 points). Tired of always doing Lagrange interpolation by hand, you stumble across someone's (poorly documented) code to do it for you. However, to your frustration, you find that it has an off-by-one error! For example, if you give it the points $(1, 3)$, $(2, 2)$, and $(3, 4)$, it would instead interpolate the points $(1, 4)$, $(2, 3)$, and $(3, 5)$ (formally, when asked to interpolate a polynomial over $GF(p)$ through some point (x, y), it will instead interpolate a polynomial through $(x, y + 1)$).
But being the clever hacker that you are, you realize that, without touching any of the code itself, for any $g(x)$ that the program returns, you can find a new polynomial $p(x)$ that is the one you originally wanted.

Describe how to construct $p(x)$ using $g(x)$. Justify your answer.

(Specifically, we are asking: given a polynomial $g(x)$ of degree $n-1$ over $GF(p)$ through points $(x_1, y_1 + 1), (x_2, y_2 + 1), \ldots, (x_n, y_n + 1)$, find a polynomial $p(x)$ of degree $n - 1$ over $GF(p)$ through points $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$).

6.3 (10 points). After fiddling with the program in part 6.2 you end up with the following quadratic (degree 2) polynomials over $GF(p)$:

$w_1(x)$ which passes through the points $(1,3), (2,1),$ and $(3,1)$

$w_2(x)$ which passes through the points $(1,1), (2,2),$ and $(3,1)$

$w_3(x)$ which passes through the points $(1,1), (2,1),$ and $(3,4)$

Describe how to use these polynomials to find the quadratic polynomial $p(x)$ over $GF(p)$ that passes through the points $(1,3)$, $(2,2)$, and $(3,4)$. Express your answer in terms of $w_1(x)$, $w_2(x)$, and $w_3(x)$.