EECS 70 Discrete Mathematics and Probability Theory
Spring 2013 Anant Sahai

MT 1

Problem 1. Stable Marriage (20 points)

(a) (5 points) Assume that there are three men 1, 2, and 3 and three women A, B, and C. Their preference lists are given below.

Man	Preference List
1	$A > C > B$
2	$A > B > C$
3	$C > A > B$

Woman	Preference List
A	$3 > 1 > 2$
B	$2 > 3 > 1$
C	$1 > 2 > 3$

Is the pairing $\{(1,C),(2,A),(3,B)\}$ stable? Why?

(b) (5 points) **Run the traditional propose and reject algorithm on the example above and write down the pairing that is produced.** Show your work (i.e. the intermediate steps of the algorithm).

(c) (10 points) Karl and Emma are having a disagreement regarding the traditional propose-and-reject algorithm. They both agree that it favors men over women. But they disagree about what, if anything, can be done without changing the ritual form of men proposing, women rejecting, and people getting married when there are no more rejections.

Karl mansplains: "It's hopeless. Men are obviously going to propose in the order of their preferences. It's male optimal so why would they do anything else? As far as the women are concerned, given that they face a specific choice of proposals at any given time, they are obviously going to select the suitor they like the most. So unless we smash the system entirely, it is going to keep all women down."

Emma says: "People are more perceptive and forward-looking that you think. Women talk to each other and know each other's preferences regarding men. They can also figure out the preferences of the men they might be interested in. A smart and confident woman should be able to do better for herself in the long run by not trying to cling to the best man she can get at the moment. By rejecting more strategically, she can simultaneously help out both herself and her friends."

Is Emma ever right? If it is impossible, prove it.

If it is possible, **construct and analyze an example (a complete set of people and their preference lists) in which a particular woman acting on her own (within the traditional ritual form of men proposing and women rejecting) can get a better match for herself while not hurting any other woman.** Show how she can do so. The resulting pairing should also be stable.

Problem 2. [True or false] (48 points)

Circle TRUE or FALSE.

Prove all statements that you think are true and disprove (e.g. by showing a counterexample) all statements that you think are false.

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

(a) TRUE or FALSE: Suppose that P, Q are propositions, $(\neg(P \Rightarrow Q))$ is logically equivalent to $(Q \Rightarrow P)$.

(b) TRUE or FALSE: Consider the Fibonacci numbers

$$F(n) = \begin{cases} 0 & \text{if } n = 0 \\ 1 & \text{if } n = 1 \\ F(n-1) + F(n-2) & \text{if } n \geq 2 \end{cases}$$

$F(n)$ is even if and only if n is a multiple of 3.

(c) TRUE or FALSE: If $a \in \mathbb{N}$ and $m \in \mathbb{N}$ are such that $0 < a < m$ and $\gcd(a, m) = 1$, then $a^{m-1} = 1 \mod m$.

(d) TRUE or FALSE: If n is an integer and $n^3 + 5$ is odd then n is even.

(e) TRUE or FALSE: $a \equiv b \mod m \Longrightarrow a^x \equiv b^x \mod m$ (assume that a, b, m, and x are all positive integers)

(f) TRUE or FALSE: $a \equiv b \mod m \Longrightarrow x^a \equiv x^b \mod m$ (assume that a, b, m, and x are all positive integers)

Problem 3. RSA. (45 points)

Rather than doing traditional RSA based on two prime numbers, suppose that your friend suggests using three prime numbers. She decides to use $N = 105 = 3 \cdot 5 \cdot 7$ and selects $e = 5$ so that the public key is $(N, e) = (105, 5)$.

(a) (4 points) **Encrypt the message** 2 **using this public key.**

(b) (6 points) **Encrypt the message** 3 **using this public key.**

(c) (15 points) **What property should the secret key** d **satisfy? Calculate what you think the secret key** d **should be for this public key** $(N = 105, e = 5)$**.** Explain your reasoning and show your work.

It is alright if you don't prove that this is the right property, proofs are required in the next part. No proofs needed in part c.

d = _____

(d) (20 points) **Prove that the encryption function** $E(x) = x^e \mod N$ **and the decryption function** $D(y) = y^d \mod N$ **above are inverses.** (i.e. $\forall x, (0 \leq x < N) \Rightarrow (D(E(x)) = x)$.)

(HINT: Follow the RSA proof from class and just adapt it for when there are three primes involved.)