CS 70 Discrete Mathematics and Probability Theory
Summer 2011 Kamil HW 3

Due Tuesday, July 5, 4:59pm

1. (12 pts.) Stable marriage

(a) Consider the following instance of the stable marriage problem:

Man	highest→lowest		
1	*B*	*A*	*C*
2	*C*	*B*	*A*
3	*A*	*C*	*B*

Table 1: Men's preference list

Woman	highest→lowest		
A	1	2	3
B	2	3	1
C	3	1	2

Table 2: Women's preference list

(i) List the rogue couples in the pairing $\{(1,C),(2,B),(3,A)\}$.

(ii) List **all** the possible stable pairings (note that a single run of the algorithm from class will only reveal one; there may be others).

(b) Run the "propose and reject" algorithm on the following example:

Man	highest→lowest			
1	*B*	*C*	*A*	*D*
2	*C*	*A*	*B*	*D*
3	*A*	*B*	*C*	*D*
4	*B*	*C*	*A*	*D*

Table 3: Men's preference list

Woman	highest→lowest			
A	4	1	2	3
B	2	3	4	1
C	3	4	1	2
D	1	2	3	4

Table 4: Women's preference list

Use the same notation as in Note 4, page 30, to illustrate the operation of your algorithm at each stage of the process. Show clearly the final stable pairing produced by your algorithm.

2. (15 pts.) Stable Marriage True-or-False?
For each of the following claims, state whether the claim is true or false. If it is true, give a *short* proof; if it is false, give a *simple* counterexample.

(a) In a stable marriage instance, if man M and woman W each put each other at the top of their respective preference lists, then M must be paired with W in every stable pairing.

(b) In a stable marriage instance with at least two men and two women, if man M and woman W each put each other at the bottom of their respective preference lists, then M cannot be paired with W in any stable pairing.

(c) For every $n > 1$, there is a stable marriage instance with n men and n women which has an unstable pairing in which every unmatched man-woman pair is a rogue couple.

3. (9 pts.) Man-Optimal, Woman-Optimal

In a particular instance of the stable marriage problem with n men and n women, it turns out that there are exactly three distinct stable pairings, $\mathscr{P}_1, \mathscr{P}_2, \mathscr{P}_3$. Also, each woman W has a different partner in the three pairings. Therefore, each woman has a clear preference ordering of the three pairings (according to the ranking of her partners in her preference list). Now, suppose that for woman W_1 this order is $\mathscr{P}_1 > \mathscr{P}_2 > \mathscr{P}_3$. True or false: every woman has the same preference ordering $\mathscr{P}_1 > \mathscr{P}_2 > \mathscr{P}_3$. Justify your answer carefully, using facts about Stable Marriage that we proved in class.

4. (12 pts.) Modular Arithmetic

(a) Give the addition and multiplication tables for modular-5 arithmetic. Write down the inverse for each of the elements which have one, and identify the ones which have no inverse.

(b) Solve the following equations for x and y or show that no solution exists. Show your work (in particular, what division must you carry out to solve each case).

(i) $5x + 23 \equiv 6 \pmod{47}$

(ii) $9x + 80 \equiv 2 \pmod{81}$

(iii) The system of simultaneous equations
$30x + 3y \equiv 0 \pmod{37}$ and $y \equiv 4 + 13x \pmod{37}$

(c) Compute $\gcd(5688, 2010)$ and show your steps.

(d) Use Extended Euclid's algorithm to find some pair of integers j, k such that $52j + 15k = 3$. Show your work.

5. (10 pts.) GCD

In class we saw that, if $\gcd(m,x) = 1$ then there are m distinct elements in the set $\{\bmod(ax,m) : a \in \{0,\ldots,m-1\}\}$. If $gcd(m,x) > 1$, how many distinct elements are there? Prove your answer.

6. (10 pts.) Modular arithmetic proof

Give a proof to the following theorem. You will likely find the use of modular arithmetic useful.

Theorem. If $a_1,\ldots,a_n$ is a sequence of n integers (not necessarily distinct), prove that there is some nonempty subsequence whose sum is a multiple of n.

7. (10 pts.) Poker mathematics

A *pseudorandom number generator* is a way of generating a large quantity of random-looking numbers, if all we have is a little bit of randomness (known as the *seed*). One simple scheme is the *linear congruential generator*, where we pick some modulus m, some constants a, b, and a seed x_0, and then generate the sequence of outputs $x_0, x_1, x_2, x_3, \ldots$ according to the following equation:

$$x_{t+1} = \bmod(ax_t + b, m)$$

(Notice that $0 \le x_t < m$ holds for every t.)

You've discovered that a popular web site uses a linear congruential generator to generate poker hands for its players. For instance, it uses x_0 to pseudo-randomly pick the first card to go into your hand, x_1 to pseudo-randomly pick the second card to go into your hand, and so on. For extra security, the poker site has kept the parameters a and b secret, but you do know that the modulus is $m = 2^{31} - 1$ (which is prime).

Suppose that you can observe the values x_0, x_1, x_2, x_3, and x_4 from the information available to you, and that the values $x_5, \ldots, x_9$ will be used to pseudo-randomly pick the cards for the next person's hand. Describe how to efficiently predict the values $x_5, \ldots, x_9$, given the values known to you.

8. (12 pts.) RSA

In this problem you play the role of Amazon, who wants to use RSA to be able to receive messages securely.

(a) Amazon first generates two large primes p and q. He picks $p = 13$ and $q = 19$ (in reality these should be 512-bit numbers). He then computes $N = pq$. Amazon chooses e from $e = 37, 38, 39$. Only one of those values is legitimate, which one? (N, e) is then the public key.

(b) Amazon generates his private key d. He keeps d as a secret. Find d. Explain your calculation.

(c) Bob wants to send Amazon the message $x = 102$. How does he encrypt his message using the public key, and what is the result?

(d) Amazon receives an encrypted message $y = 141$ from Charlie. What is the unencrypted message that Charlie sent him?

9. (10 pts.) Easy RSA

In class, we said that RSA uses as its modulus a product of two primes. Let's look at a variation that uses a single prime number as the modulus. In other words, Bob would pick a 1024-bit prime p and a public exponent e satisfying $2 \leq e < p - 1$ and $\gcd(e, p - 1) = 1$, calculate his private exponent d as the inverse of e modulo $p - 1$, publish (e, p) as his public key, and keep d secret. Then Alice could encrypt via the equation $E(x) = \bmod(x^e, p)$ and Bob could decrypt via $D(y) = \bmod(y^d, p)$.

Explain why this variation is insecure. In particular, describe a procedure that Eve could use to recover the message x from the encrypted value y that she observes and the parameters (e, p) that are known to her. Analyze the running time of this procedure, and make sure to justify why Eve could feasibly carry out this procedure without requiring extravagant computation resources.