CS007 **Fall 1997**

Homework #4

Out : September 30, 2:30 pm 1997
Due : October 7, 12:30 pm 1997

1. Say for each of the following pairs of numbers whether or not the two numbers are relatively prime.

   (a) 18, 4

   (b) 7, 27

   (c) 24, 33

   (d) 22, 51

   (e) 0, 17

2. For each of the following numbers, n, list the nonnegative numbers less than n that are relatively prime to n, and use this list to find $\phi(n)$.

   (a) 18

   (b) 23

   (c) 77

   (d) 16

   (e) 15

3. While you are at the racetrack, a jockey friend of yours slips you a piece of paper with the results of five trial races run yesterday with the four horses in today's race. Unfortunately, you have forgotten what they key you agreed upon was (although you do remember that it was chosen uniformly at random). You know that the message was encrypted using the following function:

		plain (Horse)			
		0 (Lucky Charms)	1 (Greased Lightning)	2 (Eight Ball)	3 (Great Scott)
	0	0	1	2	3
	1	1	2	3	0
	2	2	3	0	1
key	3	3	0	1	2
	4	2	3	0	1
	5	2	3	0	1
	6	2	3	0	1
	7	2	3	0	1

   Consider the information you can get by decrypting his message, “33333”.

   (a) Given this cyphertext, what are the possible combinations of winning horses?

   (b) Which horse do you bet on in today's race? Why?

4. Each employee in your company has chosen a password for logging in to the computer system. Recently, your company has decided that each employee's password should be secret-shared among two other employees, just in case. Each password can be represented by a number from 0 to 9999. Your job is to choose the secret-sharing scheme. You can assume that the two employees holding shares of their co-worker's key will not collaborate to determine the key except in an official emergency. You consult with your three underlings, Larry, Moe, and Curly...

   - Larry says:

     > "For each secret password s to be shared, choose a random number b uniformly from 0 to 9999. The number b is the first share. Let $c = s - b \pmod{10000}$. The number c is the second share."

   - Moe says:

     > "I agree with Larry's suggestion except for one thing. If the random number b is 0, the share c is the same as the secret. That's not very secure! I therefore propose that the number b be chosen uniformly from 1 to 9999 instead of from 0 to 9999."

   - Curly says:

     > "I agree with Moe's suggestion except for one thing. If the random number b is less than 10, then the share c will probably have the same hundreds place digit and the same thousands place digit as the secret s. That's not very secure! I therefore propose that the number b be chosen uniformly from 10 to 9999."

   Whose scheme is most secure, and why? Consider in particular how much the person receiving the share c thereby learns about the secret s.

5. In order that that the secret combination to the CS007 safe would be available in an emergency situation, the TA's have each been given part of the secret. The secret consists of four mod-7 blocks. For each of these numbers, Prof. Klein chose a mod-7 line—the slope of the line is the secret number and the y-intercept was chosen randomly. Prof. Klein then provided each TA with an (x, y) point on each of the lines. Thus Kevin Ingersoll got a point on each of the four lines (namely the points with x-coordinate 1), Kevin Sikorski got a point on each of the four lines (namely the point with x-coordinate 2), and Sheryl got a point on each of the four lines (with x-coordinate 3). Due to a security slip-up, you happen upon a few of the y-coordinates, as shown in the following table.

	1st block	2nd block	3rd block	4th block
Kevin Ingersoll ($x = 1$)	4	6		2
Kevin Sikorski ($x = 2$)	2		1	
Sheryl ($x = 3$)		3	1	

(a) For each block of the secret that can be determined from the information given you, give us the block, showing your work.

(b) For each block of the secret that cannot be determined from the information you have, tell us why it cannot be determined and tell us what possible values that block has.