M. Tech (CSE-ISE) Number Theory and Cryptography (CS800)

Lab Assignment-3 (Week-5: 07.09.2018)

(**Topic:** Congruence of Numbers)

A. Write a MATLAB program to:

a) Calculate the day of the week for any calendar date.

Input Format

DD/MM/YYYY

b) Find an integer k, such that a^k≡b(mod m),

where a and m are relatively prime.(Using appropriate theorem)

If it is not possible for any k to satisfy this relation, print -1.

Input Format

a,b,m

c) Find an integer x, such that ax≡b (mod m),

where a and m are relatively prime.

If it is not possible for any x to satisfy this relation, print -1.

Input Format

a,b,m

d)We are given two arrays num[0..k-1] and rem[0..k-1].

In num[0..k-1], every pair is coprime (gcd for every pair is 1).

We need to find minimum positive number x such that:

x mod num[0] = rem[0],

x mod num[1] = rem[1],

....

x mod num[k-1] = rem[k-1]

Input Format

Input: num[] = {5, 7}, rem[] = {1, 3}

e)Build Pseudo Random Number Generator using simple modulo operation.

Input Format

seed value(String)

f) Find a^k(mod b) (Using appropriate theorem).

Input Format

a,k,b

g) Find last two digit of any given expression (Using appropriate theorem).

Input Format

a,k

Example: 25^10+5*6

h) Monk likes to experiment with algorithms. His one such experiment is using modulo in sorting. He describes an array modulo sorted as: Given an integer k, we need to sort the values in the array according to their modulo with k. That is, if there are two integers a and b, and a%k<b%k, then a would
come before b in the sorted array. If a%k=b%k , then the integer which comes first in the given array
remains first in the sorted array.

Input Format

The first line consists of two integers N and k, N being the number of elements in the array and k is the number with which we need to take the modulo.

The next line consists of N space separated integers , denoting the elements of the array A.

i) Reduce the following congruences to the form of $x^2 = a$ (mod p).

1) $a_1 x^2 + b_1$ x+ c_1 =p(mod m)

j) Find solutions :

1) $x^2 = p_1$ (mod m_1)

2)$x^2 = p_2$ (mod m_2)

B. Note:

1. Write your MATLAB program as a function with its manual page.

2. Proper indentation with comments is mandatory.

3. Upload your source code (.m) with the name **<rollno>-<qno>.m** (<qno> is the assigned question no. and <rollno> is the roll no. of the respective student, eg. 182257) and a snapshot of the result as **<rollno>-<qno>.png** at brc.nitk.ac.in

C. Program to be executed:

Sl.No.	**Q**	**Sl. No.**	**Q**	**Sl. No.**	**Q**	**Sl. No.**	**Q**	**Sl. No.**	**Q**
1	a, f	6	b,g	11	c, h	16	d, j	21	e, f
2	f, b	7	c, h	12	h, a	17	d, f	22	j,c
3	j, e	8	a, i	13	e,g	18	g, b	23	g,a
4	c, f	9	d, j	14	b,j	19	f,c	24	h,d
5	d, h	10	e, i	15	a,f	20	a,h	25	b, h

***** Best of Luck *****