M. Tech (CSE-ISE) Number Theory and Cryptography (CS800)
Lab Assignment-3 (Week-6: 07.09.2018)
(Topic: Congruence of Numbers)

A. Write a MATLAB program to:

a)Julius Caesar protected his confidential information by encrypting it using a cipher. Caesar's cipher shifts each letter by a number of letters. If the shift takes you past the end of the alphabet, just rotate back to the front of the alphabet. In the case of a rotation by 3, w, x, y and z would map to z, a, b and c.
Note: The cipher *only* encrypts letters; symbols, such as -, remain unencrypted

Input Format

The first line contains the integer, , the length of the unencrypted string.

The second line contains the un-encrypted string, .

The third line contains , the number of letters to rotate the alphabet by.

Output Format

For each test case, print the encoded string.

b)**Implementation of Affine Cipher:**
The encryption function for a single letter is
Encryption:
E(x)=(ax+b) mod m
Modulus m: size of the alphabet
a and b: key of the cipher
a must be chosen such that a and m are coprime.

Decryption:
D(x)=a^-1(x-b) mod m
a^-1:modular multiplicative inverse of a mod m i.e 1=a a^-1 mod m

c)Alex has started hacking websites, and also started learning encryption and decryption of messages. Once he faced an interesting issue, where he needs to decrypt the message in a different way.

Initially, he will be given an array *A* of *N* integers, and has to decrypt *Q* messages. In each message he will get an integer *X*, and if *X* can be converted into product of two different or same prime numbers, then the real message is "YES" (without quotes), otherwise the message is "NO" (without quotes).
To convert *X*, he can choose one element from array say *Y* (*X* should be divisible *Y*), and can divide *X* by *Y* any number of times (till *X* is divisible by *Y*). Help Alex in decrypting the messages.

Input Format:

First line will contain an integer *N* and *Q*,, denoting the number of elements in the array and number of encrypted messages respectively.

Next line will contain *N* space-separated integers representing the elements of the array.

In next *Q* lines, each line will contain an integer *X* , representing an encrypted message.

Explanation

For X=16,

We can choose *2* from the given array and divide *X* by *2* , two times, which will result in *4*.

As, 4=2×2. So answer is YES.

For X=429, we can't choose any number from the array by using which we can convert *X* in product of two primes. So answer is NO.

For X=42,

We can choose *2* from the given array and divide *X* by *2* only one time, which will result in 21.

As, 21=7×3. So answer is YES.

d)An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?

Input Format: Number of egg remains in each case, will be provided at run time.

Output Format: Smallest number of eggs, that a lady could have.

e)A dragon has N heads. A knight can cut off a1, b1, c1, or d1 heads, respectively, with one blow of his sword. In each of these cases a2, b2, c2, or d2 new heads grow on its shoulders, respectively. If all heads are blown off, the dragon dies. Can the dragon ever die for your input?
Input format: N,a1,b1,c1,d1,a2,b2,c2,d2
Output format: yes/no

f) Write a MATLAB code to find n-digit (decimal) number which leaves a remainder of r when divided by 7, 9 or 11.
Input Format: Given n.
Output Format: n digit number satisfy the given condition

g)Write a MATLAB code to find the remainder when a!b! is divided by c.

h)Write a MATLAB code use the Sieve of Eratosthenes to find all primes less than n, where n is some positive integer.

i)Write a MATLAB code to display all the primitive roots of n using appropriate theorems.

j)Write a MATLAB code to find and display the reduced residue system modulo a^m , where, a and m are positive integers.

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 -.m (is the assigned question no. and is the roll no. of the respective student, eg. 182257) and a snapshot of the result as -.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 ***