# Problem A. Chinese Theorem

Input file: standard input
Output file: standard output

Time limit: 1 second Memory limit: 256 mebibytes

Find an integer solution x to the following system of equations:

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m}, \end{cases}$$

where n and m are coprime. If there are multiple solutions, find the one where x is non-negative and minimal.

### Input

The input file contains 4 integers a, b, n and m  $(1 \le n, m \le 10^6, 0 \le a < n, 0 \le b < m)$ .

# Output

Output a single integer – the solution x.

standard input	standard output
1 0 2 3	3
3 2 5 9	38

# Problem B. Consecutive Remainders

Input file: standard input
Output file: standard output

Time limit: 1 second Memory limit: 256 mebibytes

Alice and Bob playing with numbers today!

Alice says three numbers p, a, b. p, as you may guess, is prime.

Bob, on his turn, want to find integer  $0 \le x < p$  such that  $(x+b)^a \equiv x^a \mod p$ . But finding just one such number is boring, so Bob wants to find few such numbers.

If there are less than 10 such x, print all of them. Else print 10 different x, satisfying equation above.

#### Input

Input contains t testcases. Each testcase given in separate line. Input follows format:

 $p_1a_1b_1$ 

 $p_t a_t b_t$ 

. . .

 $1 \leqslant t \leqslant 10^4, \ 2 \leqslant p_i \leqslant 10^9 + 7, \ 0 \leqslant a_i \leqslant 10^9, \ 0 \leqslant b_i < p_i.$ 

### Output

For each testcase, output number of integers you have found. Then output found integers.

standard input	standard output
3	4
11 5 3	1 7 9 10
13 5 4	0
7 4 1	
	1
	3

# Problem C. Count the Sequences

Input file: standard input
Output file: standard output

Time limit: 1 second Memory limit: 256 mebibytes

For given prime number p find the number of different sequences of positive integers  $a_0, a_1, \ldots$  that satisfy the equation

$$\frac{a_0}{a_1} + \frac{a_0}{a_2} + \ldots + \frac{a_0}{a_i} + \frac{p}{a_{i+1}} = 1$$

for any positive integer i. Also find sum of n-th terms of all such sequences.

# Input

First line contains two integers p, n, separated by a space,  $0 \le n \le 10^9$ ,  $2 \le p \le 10^9$ , p - prime.

# Output

In the first line output two numbers separated by a space — the number of required sequences and the sum of n-th terms of this sequences. Output answer modulo  $10^9 + 7$ . In case of infinite number of such sequences output two -1's.

standard input	standard output
666013 25	24 660004499

#### Numbers Theory Caribbean Camp, Thursday, March 15, 2018

# Problem D. Diophantine Equation

Input file: standard input
Output file: standard output

Time limit: 1 second Memory limit: 256 mebibytes

You're given three integers a, b and c. Find an integer solution to the equation ax + by = c. If there are multiple solutions, find the one where x is non-negative and minimal.

### Input

The first and only line contains 3 integers a, b and c  $(1 \le a, b, c \le 10^4)$ .

### Output

Output x and y on a single line separated by a space. If a solution does not exist, then output «Impossible».

standard input	standard output
1 2 3	1 1

#### Numbers Theory Caribbean Camp, Thursday, March 15, 2018

# Problem E. Division

Input file: standard input
Output file: standard output

Time limit: 1 second Memory limit: 256 mebibytes

You are given 2 integers a and b,  $b \neq 0$ . The quotient of dividing a by b is  $q = \lfloor a/b \rfloor$  (brackets denote the integer part). The remainder of the division is r = a - qb. It's easy to show that if b > 0, then  $0 \leq r < b$ . Conversely, if b < 0, then  $b < r \leq 0$ . You are given 2 integers a and b, find the quotient and the remainder when dividing a by b.

#### Input

The input contains 2 integers a and b ( $|a|, |b| \le 10^8$ ).

### Output

Output 2 space-separated integers -q and r. If a solution cannot be found, then output «Impossible» (without quotes)).

standard input	standard output
10 9	1 1
-10 -9	1 -1

# Problem F. Calculate the Function

Input file: standard input
Output file: standard output

Time limit: 1 second Memory limit: 256 mebibytes

You're given a number N. Calculate the following functions:

 $\varphi(N)=$  the number of numbers in  $1,2,\ldots,N$  which are coprime with N  $\tau(N)=$  the number of divisors of N  $\sigma(N)=$  the sum of divisors of N

# Input

The input contains a single integer  $1 \le N \le 10^9$ .

### Output

On the first line output 3 space-separated integers – the values of  $\varphi(N)$ ,  $\tau(N)$  and  $\sigma(N)$  respectively.

standard input	standard output
2	1 2 3

# Problem G. Multiplicative Inverse

Input file: standard input
Output file: standard output

Time limit: 1 second Memory limit: 256 mebibytes

The multiplicative inverse of n modulo m is an integer x such that  $nx \equiv 1 \pmod{m}$ .

### Input

The input contains 2 integers n and m  $(1 \le n, m \le 10^9)$ .

### Output

Output a single integer – the multiplicative inverse of n modulo m. If a solution doesn't exist, output -1.

standard input	standard output
1 2	1
1 5	1
2 4	-1

# Problem H. Permutation Game

Input file: standard input
Output file: standard output

Time limit: 3 seconds Memory limit: 256 mebibytes

Little Petya likes permutations of numbers 1, 2, ..., N a lot. Recently he has received one as a gift from his mother. The only thing Petya likes more than permutations is playing with little Masha. She also has a permutation of the first N positive integers.

Children are playing the following game. Before beginning of the game, a permutation 1, 2, ..., N is written on the board. Players alternate turns. Masha moves first. On each turn, a player applies his permutation to the one written on the board. The whole game lasts for T turns. Petya wrote down the permutation which was left on the board after the last turn.

The result of applying a permutation A to a permutation B is the permutation C which satisfies the following condition:  $C_i = B_{A_i}$  for all i between 1 and N, inclusive.

Years have passed since then. Petya has been keeping his permutation for all the time passed. Now Petya is wondering whether it is possible to deduce Masha's permutation knowing the one he wrote down after the game and his own permutation. If there are several permutations which could have been owned by Masha, he will accept any of them. There is a possibility that Petya has mistaken when writing down a permutation from the board, which means that no permutation would lead to such game results.

#### Input

The first line of input contains two integer numbers N ( $1 \le N \le 10^6$ ) and T ( $1 \le T \le 2 \cdot 10^9$ ). Each one of the second and the third lines contains a permutation of numbers 1, 2, ..., N — Petya's permutation and the permutation which was left on the board after the game ended, respectively.

## Output

If there is no permutation which could have been owned by Masha, output a single number "-1" (without quotes). Otherwise, output such permutation in the same format as it shown in sample tests. If there are several permutations which satisfy the above conditions, you may output any of them.

standard input	standard output
5 2	2 3 1 4 5
1 2 3 5 4	
2 3 1 5 4	

# Problem I. Multiplicative Functions

Input file: standard input
Output file: standard output

Time limit: 1 second Memory limit: 256 mebibytes

In number theory, a multiplicative function is an arithmetic function F(n) of the positive integer n with property that F(1) = 1 and whenever a and b are coprime  $(\gcd(a, b) = 1)$ , then F(ab) = F(a)F(b).

The function E(n) defined by E(n) = 1 if n = 1 and = 0 if n > 1, is sometimes called multiplication unit for Dirichlet convolution or simply the unit function. If F and G are two multiplicative functions, one defines a new multiplicative function F \* G, the Dirichlet convolution of F and G, by

$$(F * G)(n) = \sum_{d|n} F(d)G\left(\frac{n}{d}\right),$$

where the sum extends over all positive divisors d of n. With this operation, the set of all multiplicative functions turns into an abelian group; the identity element is E.

(from Wikipedia, the free encyclopedia)

In this task you have to find the inverse of a multiplicative function. To cope with overflow problem, we define arithmetic functions as:  $F: \mathbb{N} \to \mathbb{Z}_{2007}$  where  $\mathbb{N}$  is the set of positive integers, and  $\mathbb{Z}_{2007}$  is a residue ring (ring of integers 0–2006, where arithmetic operations + and × are performed modulo 2007). Function G is called the inverse of function F if and only if:

$$F * G = G * F = E$$

You are given the first N values of function F, you need to find the first N values of the inverse function G.

#### Input

In the first line of the input one number N is written  $(1 \le N \le 10^4)$ . In the second line values F(1) F(2)  $F(3) \dots F(N)$  are listed. Numbers are separated by spaces. (Each value is nonnegative and doesn't exceed 2006.)

## Output

In the first line of the output print first N values of inverse function G, separated by spaces: G(1) G(2)... G(N). You should output all numbers in one line.

standard input	standard output
16	1 2006 2006 0 2006 1 2006 0 0 1 2006
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	0 2006 1 1 0

# Problem J. Not Fast Fourier Transform

Input file: standard input
Output file: standard output

Time limit: 2 seconds Memory limit: 256 mebibytes

Set  $P = 4066273 = 2016 \cdot 2017 + 1$  — prime number. All calculations are modulo P. Integer g = 5 is primitive root modulo P.

Assume  $A(x) = \sum_{i=0}^{n-1} a_i x^i$  is a polynomial with integer coefficients. Find values  $A(1), A(g), A(g^2), \ldots, A(g^{n-1})$ . You have to find the sum of this numbers.

#### Input

The first line contains one integer n ( $1 \le n \le 200\,000$ ). The second line contains n integers  $a_i$  — coefficients of the polynomial A ( $0 \le a_i < P$ ).

### Output

Output single integer  $\sum_{k=0}^{n-1} A(g^k)$  modulo P.

standard input	standard output
2	14
1 2	

#### Numbers Theory Caribbean Camp, Thursday, March 15, 2018

# Problem K. Number of Solutions

Input file: standard input
Output file: standard output

Time limit: 1 second Memory limit: 256 mebibytes

How many solutions has the equation  $X^2 - \lfloor X^2 \rfloor = \{X\}^2$  in the interval [A;B]?

# Input

The only line contains two integers A and B, separated by a space,  $0 \le A \le B \le 10^9$ .

# Output

Output one integer — number of solutions of equation in the interval [A; B] modulo  $10^9 + 7$ . If there is infinitive number of solutions output -1.

standard input	standard output
4 4	1

# Problem L. Breaking RSA

Input file: standard input
Output file: standard output

Time limit: 2 seconds Memory limit: 256 mebibytes

In 1977 Ronald Linn Rivest, Adi Shamir and Leonard Adleman proposed new cryptographic scheme RSA, still used nowadays. RSA is open-key cryptographic scheme: anybody, who knows open key, can encrypt a message, but decryption is only available for owners of secret key.

For RSA you need to generate two distinct prime numbers p and q, calculate n = pq, and generate two numbers e and d such that  $ed \equiv 1 \pmod{(p-1)(q-1)}$  (note that  $(p-1)(q-1) = \varphi(n)$ ). The pair (n,e) is open key and known to everybody. Integer d is the secret key. Also prime decomposition of n should be secret, because it allows to find d using open key.

Messages in RSA are elements of  $\mathbb{Z}_n$ . Say M is a message. Then  $C = M^e \mod n$  is encryption of M. To decrypt message, one need to calculate  $C^d \mod n = M$ .

You have encrypted message C and open key: integers n and e. Find decryption of message C.

### Input

The first line contains three integers:  $n, e, C, n \leq 10^9, e \leq 10^9, C < n$ . It is guranteed that n and e are part of some RSA system, meaning n is product of two distinct primes and e is coprime with  $\varphi(n)$ . Integer C is result of encryption of some message M.

## Output

Output one integer M ( $0 \le M < n$ ), which is decryption of C.

standard input	standard output
143	123
113	
41	
9173503	111111
3	
4051753	

# Problem M. Kinan and Pairs

Input file: standard input
Output file: standard output

Time limit: 2 seconds Memory limit: 256 mebibytes

Once upon a time Kinan came up with following problem:

You are given integers a and b. You can to three types of actions with this integers

- add one integer to the other
- substract one integer from the other
- swap a and b

Your task is to obtain pair (c, d) from pair (a, b).

Please, help Kinan to solve the problem.

#### Input

First line contains 4 integers a, b, c, d, separated by space  $(|a|, |b|, |c|, |d| \le 10^6)$ .

### Output

If there is no solution, output «No solution.». Otherwise output nubmer of actions in the first line, then actions in separate line in the form «a += k \* b \*, «b += k \* a \*, «a -= k \* b \*, «b -= k \* a \*, «swap(a, b)». Integer k denotes number of times you repeat the operation.

Number of actions in output should be no more that 10000. All intermediate results should have absolut value no more that  $10^9$ . It is guaranteed that if solution exists, there is a solution satisfying constraints above.

standard input	standard output
1 2 3 5	2
	a += 1 * b b += 1 * a
	b += 1 * a
5 10 10 5	1
	swap(a, b)