

#### Universidade de São Paulo

Instituto de Ciências Matemáticas e de Computação Departamento de Ciências de Computação SCC211- Lab. Alg. Avançados II

# Raízes

#### 1 Descrição

Joselino Barbacena conseguiu com um vizinho uma tralha de pescaria emprestada e foi até o Rio Pardo pescar. Só que os peixes não querem saber de morder a isca e ele pensou num outro problema de teoria dos números para matar o tempo.

Dado um inteiro x, ele quer calcular a raiz quadrada modulo p, um número primo também fornecido. A resposta correta para tal problema será um inteiro s, tal que  $s \times s$  e x têm o mesmo resto após a divisão por p. Em outras palavras, o número  $(s \times s - x)$  tem que resultar em resto igual a zero após a divisão por p. Lembre-se de que nem sempre existirá uma raiz quadrada s para alguns valores de x.

Joselino Barbacena decidiu que escreveria um programa para calcular as raízes quadradas modulo de p para todo x de 0 até (p-1), ou então reportar que a raiz quadrada correspondente não existe.

## 2 Input

A primeira linha contém o número primo p ( $2 \le p \le 10^6$ ). Lembrando que um número primo tem exatamente 2 divisores.

## 3 Output

Uma linha com p inteiros, separados por um espaço em branco, tal que o  $i^{th}$  inteiro equivale à raiz quadrada de i-1 modulo p. Todos os números devem estar entre 0 e p-1. Caso alguma raiz seja inexistentes, imprima -1. Se houver mais de uma raiz para um determinado i, imprima a menor delas.

## 4 Exemplos de Entrada e Saída

Entrada	Saída
5	0 1 -1 -1 2
Entrada	Saída
7	0 1 3 -1 2 -1 -1

#### 5 Notas

No primeiro caso temos:  $1 \times 1 \equiv 1 \pmod{5}$ ,  $2 \times 2 \equiv 4 \pmod{5}$