

### H3 – Raiz primitiva

No campo da criptografia, os números primos desempenham um papel importante. O esquema “Diffie-Hellman” permite que duas partes em comunicação troquem uma chave secreta. Este método requer um número primo  $p$  e uma raiz primitiva  $r$  de  $p$ , a qual é de conhecimento público. Para um número primo  $p$ ,  $r$  é uma raiz primitiva de  $p$  se e somente se seus expoentes  $r, r^2, r^3, \dots, r^{p-1}$  são distintos (mod  $p$ ).

Escreva um programa que, dado um número primo  $p$  e outro inteiro  $r < p$ , determine se  $r$  é uma raiz primitiva de  $p$ .

#### Entrada

A entrada começará com dois inteiros  $p$  ( $p < 2^{31}$ ) e  $n$  ( $1 \leq n \leq 100$ ), separados por um espaço e em uma única linha ( $p$  é o número primo e  $n$  é a quantidade de candidatas a raízes primitivas). As próximas  $n$  linhas contém, cada uma, uma única candidata  $r$  a raiz primitiva a ser verificada.

#### Saída

A saída deve consistir de *SIM*, se  $r$  é uma raiz primitiva, ou *NAO*, caso contrário.

#### Exemplos de entradas e saídas

Entrada:	Saída:
5 2	SIM
3	NAO
4	

  

Entrada:	Saída:
7 2	SIM
3	NAO
4	

**Comentários a respeito do primeiro caso de teste:** Dado que  $3^1, 3^2, 3^3$  e  $3^4 \pmod{5}$  são, respectivamente, 3, 4, 2 e 1; a candidata 3 é uma raiz primitiva de 5. Como  $4^1, 4^2, 4^3$  e  $4^4 \pmod{5}$  são respectivamente 4, 1, 4 e 1; então 4 não é uma raiz primitiva de 5.