Exercício 1 — Portal

O que é um inverso?

Lembre-se que um número multiplicado pelo seu inverso é igual a 1. De aritmética básica, sabemos que:

- O inverso de um número A é 1/A desde A * 1/A = 1

  por exemplo, o inverso de 5 é 1/5

- Todos os números reais diferentes de 0 têm um inverso

- Multiplicar um número pelo inverso de A é o mesmo que dividir por A

  por exemplo, 10/5 é o mesmo que 10* 1/5

O que é um inverso modular?
Em aritmética modular não temos uma operação de divisão. No entanto, temos inversos modulares.

- O inverso modular de A (mod C) é A ^ -1

- (A * A^-1) ≡ 1 (mod C) ou, de forma equivalente, (A * A^-1) mod C = 1

- Apenas os números primos de C (números que não compartilham fatores primos com C) têm um inverso modular (mod C)

Como encontrar um inverso modular
Um método simples de encontrar um inverso modular para A (mod C) é:

passo 1. Calcule A * B mod C para valores de B de 0 a C-1

passo 2. O inverso modular de A mod C é o valor de B que faz A * B mod C = 1

Perceba que o termo B mod C pode ter somente um valor inteiro entre 0 e C-1, então testar valores maiores para B é redundante.

Exemplo: A=3 C=7

Passo 1. Calcule A * B mod C para valores de B entre 0 e C-1

3 * 0 ≡ 0 (mod 7)

3 * 1 ≡ 3 (mod 7)

3 * 2 ≡ 6 (mod 7)

3 * 3 ≡ 9 ≡ 2 (mod 7)

3 * 4 ≡ 12 ≡ 5 (mod 7)

3 * 5 ≡ 15 (mod 7) ≡ 1 (mod 7) <------ ENCONTROU O INVERSO!

3 * 6 ≡ 18 (mod 7) ≡ 4 (mod 7)

Passo 2. O inverso modular de A mod C é o valor de B que faz A * B mod C = 1

5 é o inverso modular de 3 mod 7, já que 5*3 mod 7 = 1

Simples!

Vamos fazer mais um exemplo no qual não encontramos um inverso.

Exemplo: A=2 C=6Passo 1. Calcule A * B mod C para valores de B entre 0 e C-1
2 * 0 ≡ 0 (mod 6)

2 * 1 ≡ 2 (mod 6)

2 * 2 ≡ 4 (mod 6)

2 * 3 ≡ 6 ≡ 0 (mod 6)

2 * 4 ≡ 8 ≡ 2 (mod 6)

2 * 5 ≡ 10 ≡ 4 (mod 6)

Passo 2. O inverso modular de A mod C é o valor de B que faz A * B mod C = 1
Nenhum valor de B faz A * B mod C = 1. Portanto, A não tem um inverso modular (mod 6).
Isso acontece porque 2 não é primo de 6 (eles compartilham o fator primo 2).

Formato de Entrada

A primeira linha da entrada contém T, o número de casos de teste.
Cada caso de teste contém A e C.

Restrições:
1 <= T <= 1000
1 <= A <= 10000
1 <= C <= 1000

Ex:
4
7 100

19 101
10000 29
9 3

Formato de Saída

Para cada caso:
- Se A e C compartilharem fatores primos, então imprima "Caso X: muito difícil"
- Caso contrário, imprima "Caso X: Y"
Onde X é o número do caso atual, começando em 1, e Y é o inverso modular de a mod p.
Ex:
Caso 1: 43
Caso 2: 16
Caso 3: 23
Caso 4: muito difícil
//cursor aqui

Exemplos
Entrada (download):

4
7 100
19 101
10000 29
9 3

Saída (download):

Caso 1: 43
Caso 2: 16
Caso 3: 23
Caso 4: muito difícil