

## Objetivo

O objetivo desta atividade é que o aluno implemente o método para encontrar inversos multiplicativos modulares visto em sala de aula. Executamos o Algoritmo Euclidiano Estendido entre  $a$  e  $n$ , construindo a tradicional tabela com quatro colunas. Em seguida utilizamos os valores obtidos para  $d = \text{MDC}$ ,  $\alpha$  e  $\beta$  para calcular o inverso multiplicativo de  $a$  módulo  $n$ . Por exemplo, para o cálculo do inverso de 2 módulo 5, temos

R	Q	x	y
2	-	1	0
5	-	0	1
2	0	1	0
1	2	-2	1
0	2	-	-

Esta tabela será seguida então da solução: 3 é o inverso multiplicativo de 2 módulo 5.

O objetivo do programa que será realizado é ler **duplas** de números inteiros positivos e imprimir na tela para o usuário a réplica da tabela gerada, como a tabela acima, seguida, na linha abaixo, pelo inverso multiplicativo do primeiro número da dupla módulo o segundo número da dupla.

## Entrada

Inicialmente, o programa deverá ler um número inteiro  $n$ . Este número irá indicar quantas **duplas** de números inteiros positivos o programa deverá ler na sequência. Isto é, se  $n = 6$ , o programa deverá ler, em seguida, seis duplas de números inteiros positivos. Cada dupla de números será lida de uma vez, estando os dois números da dupla separados por vírgulas.

Abaixo, é apresentado um exemplo de uma possível entrada para o programa.

## Saída

Cada dupla de inteiros lida representa um inteiro e um módulo. O programa deverá imprimir uma réplica da tabela gerada pelo Algoritmo Euclidiano Estendido executado e, em seguida, na linha abaixo, o inverso multiplicativo do primeiro número da dupla módulo o segundo número da dupla. Caso o inverso multiplicativo em questão não exista, o programa deverá imprimir apenas o número 0. Após o inverso multiplicativo, o programa deverá imprimir uma linha com apenas três traços: ---.

Abaixo, é apresentado um exemplo de uma saída para o programa. Esta é justamente a saída que deve ser produzida caso o programa receba a entrada fornecida no exemplo.

## Exemplo

Este exemplo contém o caso descrito no início do enunciado.

### Entrada

```
3
2,5
2,40
3,104
```

### Saída

```
2 - 1 0
5 - 0 1
2 0 1 0
1 2 -2 1
0 2 - -
3
---
2 - 1 0
40 - 0 1
2 0 1 0
0 20 - -
0
---
3 - 1 0
104 - 0 1
3 0 1 0
2 34 -34 1
1 1 35 -1
0 2 - -
35
---
```