

## Atividade de Laboratório 8.2

Números Inteiros e Criptografia - Prof. Luis Menasché Schechter

### Objetivo

O objetivo desta atividade é que o aluno implemente o teste baseado no Teorema de Fermat visto em sala de aula que permite determinar que alguns números são compostos sem fatorá-los. Por exemplo, podemos testar o número 341 com a base 2:

$R$	$A$	$E$	$E$ é ímpar?
1	2	340	N
1	4	170	N
1	16	85	S
16	256	42	N
16	64	21	S
1	4	10	N
1	16	5	S
16	256	2	N
16	64	1	S
1	4	0	N

Vemos então que, com a base 2, o resultado do teste é inconclusivo. Testando com a base 3:

$R$	$A$	$E$	$E$ é ímpar?
1	3	340	N
1	9	170	N
1	81	85	S
81	82	42	N
81	245	21	S
67	9	10	N
67	81	5	S
312	82	2	N
312	245	1	S
56	9	0	N

Concluimos então que o número 341 é composto.

O objetivo do programa que será realizado é ler duplas de números inteiros positivos e realizar o teste baseado no Teorema de Fermat, considerando o primeiro valor da dupla como o número a ser testado e o segundo valor como a base a ser utilizada no teste. O programa deve imprimir as réplicas das tabelas geradas pelo algoritmo da potenciação utilizado no teste, seguidas dos resultados dos testes: **INCONCLUSIVO** ou **COMPOSTO**.

### 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.

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

### Saída

Para cada dupla lida, considerando o primeiro valor da dupla como o número a ser testado e o segundo valor com a base a ser utilizada no teste, o programa deverá imprimir a réplica da tabela gerada pelo algoritmo da potenciação utilizado no teste, seguida, na

linha abaixo, do resultado do teste: **INCONCLUSIVO** ou **COMPOSTO**. Após a impressão de um resultado, o programa deverá imprimir uma linha com apenas três traços: ---.

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

## Exemplo

Este exemplo é o mesmo descrito no início do enunciado.

### Entrada

2  
341,2  
341,3

### Saída

1 2 340 N  
1 4 170 N  
1 16 85 S  
16 256 42 N  
16 64 21 S  
1 4 10 N  
1 16 5 S  
16 256 2 N  
16 64 1 S  
1 4 0 N  
**INCONCLUSIVO**  
---  
1 3 340 N  
1 9 170 N  
1 81 85 S  
81 82 42 N  
81 245 21 S  
67 9 10 N  
67 81 5 S  
312 82 2 N  
312 245 1 S  
56 9 0 N  
**COMPOSTO**  
---