Atividade de Laboratório **9.1**

Números Inteiros e Criptografia - Prof. Luis Menasché Schechter

Objetivo

O objetivo desta atividade é que o aluno implemente o teste de Miller-Rabin 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. Começamos fazendo $340 = 2^2 * 85$ e então calculamos 2^{85} com auxílio do algoritmo de potenciação:

R	A	E	E é ímpar?
1	2	85	S
2	4	42	N
2	16	21	S
32	256	10	N
32	64	5	S
2	4	2	N
2	16	1	S
32	256	0	N

Por fim, calculamos $2^{2*85} \equiv (2^{85})^2 \equiv 32^2 \equiv 1 \pmod{341}$. Concluímos então que 341 é composto.

O objetivo do programa que será realizado é ler duplas de números inteiros positivos e realizar o teste de Miller-Rabin, considerando o primeiro valor da dupla como o número a ser testado e o segundo valor como a base a ser utilizada no teste.

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. Como sempre, cada dupla de números será lida de uma vez, estando os dois números da dupla separados por vírgula.

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 seguinte sequência de informações:

1. Em uma primeira linha, separados por um espaço em branco, os valores de k e q tais que o número a ser testado menos 1 é igual a $2^k * q$;

2. Em seguida, uma réplica da tabela do algoritmo de potenciação (conforme atividade 6.2) utilizando o expoente q (cálculo da primeira potência da sequência de potências do teste de Miller-Rabin);

3. Após a réplica da tabela acima, o programa deverá imprimir em uma mesma linha, separados por um espaço em branco, o expoente q e o resultado da potência calculada;

4. Caso com esta potência o resultado do teste de Miller-Rabin já seja conhecido, este resultado deve ser impresso: `INCONCLUSIVO` ou `COMPOSTO`. Após a impressão de um resultado, o programa deverá imprimir uma linha com apenas três traços: `---`;

5. Caso contrário, o programa deverá imprimir em uma mesma linha, separados por um espaço em branco, o próximo expoente da sequência de potências do teste de Miller-Rabin e o resultado desta potência. Para todas estas potências após a primeira, não é necessário o uso do algoritmo da potenciação, já que essas potências podem ser calculadas diretamente a partir das potências anteriores;

6. O programa então repete os passos 4 e 5 acima até finalizar o teste de Miller-Rabin com o resultado dele.

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

Entrada

```
3
341,2
561,2
25,7
```

Saída

```
2 85
1 2 85 S
2 4 42 N
2 16 21 S
32 256 10 N
32 64 5 S
2 4 2 N
2 16 1 S
32 256 0 N
85 32
170 1
COMPOSTO
---
4 35
1 2 35 S
2 4 17 S
8 16 8 N
8 256 4 N
8 460 2 N
8 103 1 S
263 511 0 N
35 263
70 166
140 67
280 1
COMPOSTO
---
3 3
1 7 3 S
7 24 1 S
18 1 0 N
3 18
6 24
INCONCLUSIVO
---
```