

## Objetivo

O objetivo desta atividade é utilizar o Teste de Lucas **Melhorado** para determinar se os números são primos ou compostos.

## Entrada

Inicialmente, o programa deverá ler um número inteiro  $k$ . Este número irá indicar quantos números inteiros o programa deverá ler na sequência. Isto é, se  $k = 6$ , o programa deverá ler, em seguida, seis números inteiros.

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

## Saída

Para cada inteiro  $n$  lido, o programa deverá inicialmente imprimir a tabela do algoritmo ingênuo de fatoração (conforme Atividade 4.1) exibindo a fatoração de  $n - 1$ . Em seguida, o programa deverá imprimir a base a ser utilizada no teste (o teste começará com a menor base possível e continuará com novas bases em ordem crescente, enquanto necessário). A seguir, o programa deverá imprimir o expoente da primeira potência a ser testada (as potências devem ser testadas com os expoentes na seguinte ordem:  $n - 1, (n - 1)/p_1, (n - 1)/p_2, \dots, (n - 1)/p_k$ , onde  $p_1 < p_2 < \dots < p_k$ ), seguido da tabela do algoritmo de exponenciação modular desta potência (conforme Atividade 6.2). Após esta tabela, o programa prossegue com o próximo expoente ou com a próxima base, de acordo com o que for apropriado pelo teste de Lucas. Se, em qualquer momento, o teste puder responder que o número é primo ou composto, ele deverá imprimir, respectivamente **PRIMO** ou **COMPOSTO**, seguido de uma linha com apenas três traços: ---, não devendo, portanto, realizar mais nenhuma potência. **Entretanto, ao contrário do Teste de Lucas comum, no Teste de Lucas Melhorado, é importante que todas as potências de cada base sempre sejam calculadas, para determinar quais expoentes já foram verificados de forma satisfatória com a base atual e quais precisam ser repetidos na(s) próxima(s) base(s).**

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

# Exemplo

## Entrada

2  
103  
109

## Saída

2 1  
3 1  
17 1  
2  
102  
1 2 102 N  
1 4 51 S  
4 16 25 S  
64 50 12 N  
64 28 6 N  
64 63 3 S  
15 55 1 S  
1 38 0 N  
51  
1 2 51 S  
2 4 25 S  
8 16 12 N  
8 50 6 N  
8 28 3 S  
18 63 1 S  
1 55 0 N  
34  
1 2 34 N  
1 4 17 S  
4 16 8 N  
4 50 4 N  
4 28 2 N  
4 63 1 S  
46 55 0 N  
6  
1 2 6 N  
1 4 3 S  
4 16 1 S  
64 50 0 N  
3  
102  
1 3 102 N  
1 9 51 S  
9 81 25 S  
8 72 12 N  
8 34 6 N  
8 23 3 S  
81 14 1 S  
1 93 0 N  
51  
1 3 51 S  
3 9 25 S  
27 81 12 N  
27 72 6 N  
27 34 3 S  
94 23 1 S  
102 14 0 N  
PRIMO  
---  
2 2  
3 3  
2  
108  
1 2 108 N  
1 4 54 N  
1 16 27 S  
16 38 13 S  
63 27 6 N  
63 75 3 S  
38 66 1 S  
1 105 0 N  
54  
1 2 54 N  
1 4 27 S  
4 16 13 S  
64 38 6 N  
64 27 3 S  
93 75 1 S  
108 66 0 N  
36  
1 2 36 N  
1 4 18 N  
1 16 9 S  
16 38 4 N  
16 27 2 N  
16 75 1 S  
1 66 0 N  
3  
108  
1 3 108 N  
1 9 54 N  
1 81 27 S  
81 21 13 S  
66 5 6 N  
66 25 3 S  
15 80 1 S  
1 78 0 N  
36  
1 3 36 N  
1 9 18 N  
1 81 9 S  
81 21 4 N  
81 5 2 N  
81 25 1 S  
63 80 0 N  
PRIMO  
---