Números Inteiros e Criptografia - Prof. Luis Menasché Schechter

Objetivo

O objetivo desta atividade é que o aluno implemente o Algoritmo de Fatoração de Fermat visto em sala de aula. Podemos executar este algoritmo manualmente construindo uma tabela com três colunas. Na primeira coluna, aparecem os valores sucessivos calculados para x, começando-se com a parte inteira da raiz do número a ser fatorado. Na segunda coluna, aparecem os valores sucessivos calculados para y, começando-se com zero. Já na terceira coluna, aparece a letra $\mathbb N$ (de "não") ou a letra $\mathbb S$ (de "sim"), indicando se o número a ser fatorado é ou não igual a x^2-y^2 . Por exemplo, o Algoritmo de Fatoração de Fermat irá gerar a seguinte tabela para o número 1342127:

| X | y | $n = x^2 - y^2?$ |
|------|-----|------------------|
| 1158 | 0 | N |
| 1159 | 33 | N |
| 1160 | 58 | N |
| 1161 | 76 | N |
| 1162 | 90 | N |
| 1163 | 102 | N |
| 1164 | 113 | S |

A partir da última linha da tabela, se obtém os dois fatores do número: x - y = 1051 e x + y = 1277.

O objetivo do programa que será realizado é ler números inteiros positivos **ímpares**, executar o Algoritmo de Fatoração de Fermat e imprimir na tela para o usuário a réplica das tabelas geradas, como a tabela acima, seguida dos dois fatores calculados pelo algoritmo.

Entrada

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

Abaixo, são apresentados dois exemplos de possíveis entrada para o programa.

Saída

Para cada inteiro lido, o programa deverá imprimir uma réplica da tabela gerada pelo Algoritmo de Fatoração de Fermat. A tabela deve ser construída de acordo com as instruções dadas no início do enunciado (seção "Objetivo"). Em seguida, na linha abaixo, o programa deverá imprimir os dois fatores calculados, separados por um espaço em branco. O menor fator deve ser impresso primeiro e o maior depois. Caso o inteiro lido seja primo, os fatores a serem impressos após a tabela devem ser 1 e o próprio número. Após a impressão dos fatores, o programa deverá imprimir uma linha com apenas três traços: ---.

Abaixo, são apresentados dois exemplos de saídas para o programa. Estas são justamente as saídas que devem ser produzidas caso o programa receba as entradas fornecida no exemplo.

Exemplo 1

Este exemplo é o mesmo descrito no início do enunciado.

| Entrada | Saída |
|---------|------------|
| | 1158 O N |
| | 1159 33 N |
| 1 | 1160 58 N |
| 1342127 | 1161 76 N |
| | 1162 90 N |
| | 1163 102 N |
| | 1164 113 S |
| | 1051 1277 |
| | |

Exemplo 2

| Entrada | Saída |
|--------------------|------------------------------------------------------------------------------------------------------------|
| | 11 0 N 12 4 N 13 6 N 14 8 N 15 10 S 5 25 |
| 3 | |
| 125 29 11413 | 5 0 N 6 2 N 7 4 N 8 5 N 9 7 N 10 8 N 11 9 N 12 10 N 13 11 N 14 12 N 1 29 |
| | 107 6 S 101 113 |