

Atividade de Laboratório 3.1

Números Inteiros e Criptografia - Prof. Luis Menasché Schechter

Objetivo

O objetivo desta atividade é que o aluno implemente o Algoritmo Euclidiano Estendido visto em sala de aula. Podemos executar este algoritmo manualmente construindo uma tabela com quatro colunas: a primeira que se inicia com os valores dos dois números fornecidos como entrada e, em seguida, contém os valores dos restos das sucessivas divisões realizadas pelo algoritmo; a segunda se inicia com duas casas em branco (-) e, em seguida, contém os valores dos quocientes das sucessivas divisões realizadas pelo algoritmo; a terceira se inicia com os valores 1 e 0 e, em seguida, contém os valores de x calculados pelo algoritmo; finalmente, a quarta se inicia com os valores 0 e 1 e, em seguida, contém os valores de y calculados pelo algoritmo. O valor presente na primeira coluna da última linha será zero (o algoritmo termina quando produz um resto zero) e o valor presente na primeira coluna da penúltima linha será o MDC dos dois números. Os valores nas colunas de x e de y na penúltima linha são os valores desejados de α e β . Já os valores nas colunas de x e y na última linha não são relevantes e nem são calculados (sendo colocado apenas - na tabela). Por exemplo, o Algoritmo Euclidiano Estendido entre 1234 e 54 irá gerar a seguinte tabela:

R	Q	x	y
1234	-	1	0
54	-	0	1
46	22	1	-22
8	1	-1	23
6	5	6	-137
2	1	-7	160
0	3	-	-

O objetivo do programa que será realizado é ler pares de números inteiros positivos, executar o Algoritmo Euclidiano Estendido e imprimir na tela para o usuário a réplica das tabelas geradas, como a tabela acima.

Entrada

Inicialmente, o programa deverá ler um número inteiro n . Este número irá indicar quantos pares de números inteiros positivos o programa deverá ler na sequência. Isto é, se $n = 6$, o programa deverá ler, em seguida, seis pares de números inteiros positivos. Cada par de números será lido de uma vez, estando os dois números do par separados por uma vírgula.

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

Saída

Para cada par de inteiros lido, o programa deverá imprimir uma réplica da tabela gerada pelo Algoritmo Euclidiano Estendido executado sobre os dois números do par. A tabela deve ser construída de acordo com as instruções dadas no início do enunciado (seção “Objetivo”). Repare que, nas duas primeiras linhas da coluna do quociente, deve ser impresso apenas um traço (-), assim como nas colunas de x e y da última linha. Ao final da réplica de uma tabela, 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

1
1234,54

Saída

1234 - 1 0
54 - 0 1
46 22 1 -22
8 1 -1 23
6 5 6 -137
2 1 -7 160
0 3 - -

Exemplo 2

Entrada

3
484,22
760,84
10026,168

Saída

484 - 1 0
22 - 0 1
0 22 - -

760 - 1 0
84 - 0 1
4 9 1 -9
0 21 - -

10026 - 1 0
168 - 0 1
114 59 1 -59
54 1 -1 60
6 2 3 -179
0 9 - -
