Atividade de Laboratório **14.1**

Números Inteiros e Criptografia - Prof. Luis Menasché Schechter

Objetivo

O objetivo desta atividade é "quebrar" o RSA.

Entrada

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

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

Saída

Para cada tripla lida, o primeiro elemento da tripla será o valor de n (de acordo com a notação da aula) em uma chave *pública* do RSA, o segundo elemento da tripla será o valor de e (de acordo com a notação da aula) que faz par com n na chave pública do RSA e o terceiro elemento da tripla será um bloco encriptado b no intervalo $1 < b < n$. O objetivo do programa é "quebrar" a chave pública, isto é, calcular a chave privada a partir apenas da chave pública e, com esta chave privada, decriptar o bloco b. Para isso, para cada tripla lida, o programa deverá inicialmente imprimir a tabela do Algoritmo de Fatoração de Fermat (conforme Atividade 4.2) aplicado a n, seguida, na linha abaixo, dos dois fatores obtidos (também conforme Atividade 4.2). Em seguida, o programa deverá imprimir o valor de $\phi(n)$. Após este valor, o programa deverá imprimir uma tabela do Algoritmo Euclidiano Estendido (conforme Atividade 3.1) de forma a calcular o valor de d da chave privada do RSA. Na linha abaixo, o programa deverá imprimir d, lembrando que este valor está no intervalo $1 < d < \phi(n)$. Em seguida, o programa deverá imprimir a tabela do algoritmo de exponenciação modular (conforme Atividade 6.2) utilizado para decriptar o bloco b com a chave privada (n, d). Após esta tabela, o programa deve imprimir o valor obtido para o bloco decriptado, seguido de uma linha com apenas três traços: `---`.

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

```
3
143,7,42
10403,11,199
391,3,100
```

Saída

```
11 0 N
12 1 S
11 13
120
7 - 1 0
120 - 0 1
7 0 1 0
1 17 -17 1
0 7 - -
103
1 42 103 S
42 48 51 S
14 16 25 S
81 113 12 N
81 42 6 N
81 48 3 S
27 16 1 S
3 113 0 N
3
---
101 0 N
102 1 S
101 103
10200
11 - 1 0
10200 - 0 1
11 0 1 0
3 927 -927 1
2 3 2782 -3
1 1 -3709 4
0 2 - -
6491
1 199 6491 S
199 8392 3245 S
5528 7757 1622 N
5528 97 811 S
5663 9409 405 S
9404 10154 202 N
9404 9986 101 S
463 7441 50 N
463 3715 25 S
3550 6847 12 N
3550 5491 6 N
3550 3187 3 S
5789 3641 1 S
1271 3459 0 N
1271
---
19 0 N
20 3 S
17 23
352
3 - 1 0
352 - 0 1
3 0 1 0
1 117 -117 1
0 3 - -
235
1 100 235 S
100 225 117 S
213 186 58 N
213 188 29 S
162 154 14 N
162 256 7 S
26 239 3 S
349 35 1 S
94 52 0 N
94
---
```