Atividade de Laboratório **14.3**

Números Inteiros e Criptografia - Prof. Luis Menasché Schechter

Objetivo

O objetivo desta atividade é utilizar o Algoritmo Baby-Step / Giant-Step de Shanks para resolver o Problema do Logaritmo Discreto em grupos $U(p)$, com p primo.

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 g, o segundo elemento será o valor de h e o terceiro elemento será o valor de p (primo). O objetivo é calcular o valor de x tal que $g^x \equiv h \pmod{p}$. Para cada tripla lida, o programa deverá inicialmente imprimir o valor de m, que indica a quantidade de baby-steps e giant-steps que deverão ser calculados. Em seguida, o programa deve imprimir a tabela completa dos Baby-Steps (o valor de j na primeira coluna da tabela e o baby-step correspondente na segunda coluna da tabela). A seguir, o programa deverá imprimir a tabela de giant-steps (o valor de i na primeira coluna e o giant-step correspondente na segunda coluna) até que seja encontrado o valor correto para a obtenção de x. Neste momento, os giant-steps não devem mais ser calculados. O programa deverá então imprimir os valores encontrados para i e j, em uma mesma linha, separados por um espaço. Finalmente, na linha abaixo, deverá ser impresso o valor de x, 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
3,10,199
2,73,181
6,2,151
```

Saída

```
15
0 1
1 3
2 9
3 27
4 81
5 44
6 132
7 197
8 193
9 181
10 145
11 37
12 111
13 134
14 4
0 10
1 34
2 36
3 3
3 1
46
---
14
0 1
1 2
2 4
3 8
4 16
5 32
6 64
7 128
8 75
9 150
10 119
11 57
12 114
13 47
0 73
1 176
2 102
3 55
4 145
5 119
5 10
80
---
13
0 1
1 6
2 36
3 65
4 88
5 75
6 148
7 133
8 43
9 107
10 38
11 77
12 9
0 2
1 28
2 90
3 52
4 124
5 75
5 5
70
---
```