Atividade de Laboratório 12

Números Inteiros e Criptografia - Prof. Luis Menasché Schechter

Objetivo

O objetivo desta atividade é utilizar o Algoritmo de Gauss para calcular todos os geradores de um grupo cíclico U(p), com p primo.

Entrada

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

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

Saída

Para cada primo p lido, o programa deverá inicialmente imprimir a tabela do algoritmo ingênuo de fatoração (conforme Atividade 3.2) exibindo a fatoração da ordem do grupo U(p). Em seguida, o Algoritmo de Gauss deverá ser executado. Para cada fator primo da ordem de U(p) deverá ser impressa uma linha com este fator primo e com os valores de a e b (conforme notação da aula) nas suas formas reduzidas calculados para este fator. Os três números serão impressos separados por espaços em branco. Em seguida, o programa deverá imprimir o gerador em sua forma reduzida calculado pelo algoritmo de Gauss a partir dos valores de a e b calculados anteriormente. Finalmente, na linha abaixo, o programa deverá imprimir uma lista, em ordem crescente, de **todos** os geradores do grupo U(p), obtidos a partir do gerador calculado pelo Algoritmo de Gauss. Após a impressão desta lista, o programa deverá imprimir 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	Saída
3 41 19 7	2 3 5 1 2 3 38 5 2 10 11 [6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35] 2 1 3 2 2 2 18 3 2 4 15 [2, 3, 10, 13, 14, 15]
	2 1 3 1 2 3 6 3 2 4

[3, 5]