Atividade de Laboratório 9.1

Números Inteiros e Criptografia - Prof. Luis Menasché Schechter

Objetivo

O objetivo desta atividade é que o aluno implemente o Algoritmo Chinês do Resto visto em sala de aula para resolver sistemas de congruências. Por exemplo, para resolver o sistema

$$\begin{cases} x \equiv 1 \pmod{13} \\ x \equiv 4 \pmod{15} \\ x \equiv 8 \pmod{19} \end{cases}$$

aplicamos o Algoritmo Euclidiano Estendido a 13 e 15, obtendo $\alpha=7$ e $\beta=-6$. Com isso, obtemos o valor $x\equiv 79\pmod{195}$, que satisfaz às duas primeiras congruências simultaneamente. Aplicamos então o Algoritmo Euclidiano Estendido a 195 e 19, obtendo $\alpha=4$ e $\beta=-41$. Com isso, obtemos o valor $x\equiv 274\pmod{3705}$, que é a solução do sistema.

O objetivo do programa que será realizado é ler duplas de listas de números inteiros e, considerando a primeira lista como os valores que aparecem do lado direito das congruências do sistema e a segunda lista como os módulos das congruências do sistema, aplicar o Algoritmo Chinês do Resto para solucionar os sistemas dados.

Entrada

Inicialmente, o programa deverá ler um número inteiro n. Este número irá indicar quantas **duplas** de listas de números inteiros o programa deverá ler na sequência. Isto é, se n=6, o programa deverá ler, em seguida, seis **duplas** de listas de números inteiros. Cada dupla de listas será lida de uma vez, estando as duas listas separadas por vírgula (ex: [1,4,8],[13,15,19]).

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

Saída

Para cada dupla lida, considerando a primeira lista como os valores que aparecem do lado direito das congruências do sistema e a segunda lista como os módulos das congruências do sistema, o programa deverá imprimir a seguinte sequência de informações:

- 1. Uma réplica da tabela do Algoritmo Euclidiano Estendido (conforme atividade 3.1) entre os módulos das duas primeiras congruências;
- 2. Em seguida, em uma única linha, separados por um espaço em branco, os valores calculados para α e β ;
- 3. Na linha seguinte, separados por um espaço em branco, o valor e o módulo da solução encontrada para as duas primeiras congruências;
- 4. Caso haja mais de duas congruências no sistema dado, o programa deverá então imprimir uma réplica da tabela do Algoritmo Euclidiano Estendido entre o último módulo calculado acima e o módulo da próxima congruência que ainda não foi utilizada;
- 5. O programa então repete os passos 2, 3 e 4 acima até obter a solução final (valor e módulo) para o sistema dado. Após a impressão da solução final, 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 produzidas caso o programa receba a entrada fornecidas no exemplo.

Exemplo

Entrada Saída 13 - 1 0 15 - 0 1 13 0 1 0 2 1 -1 1 1 6 7 -6 0 2 - -7 -6 79 195 195 - 1 0 19 - 0 1 5 10 1 -10 [1,4,8],[13,15,19] 4 3 -3 31 [1,0,3],[3,5,7] 1 1 4 -41 0 4 - -4 -41 274 3705 ---3 - 1 0 5 - 0 1 3 0 1 0 2 1 -1 1 1 1 2 -1 0 2 - -2 -1 10 15 15 - 1 0 7 - 0 1 1 2 1 -2 0 7 - -

1 -2 10 105