Atividade de Laboratório 14.1

Números Inteiros e Criptografia - Prof. Luis Menasché Schechter

Objetivo

O objetivo desta atividade é utilizar o Método de Fermat para encontrar fatores de Números de Mersenne.

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 deverá 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 o Número de Mersenne M(p). Na linha a seguir, o programa deverá imprimir o valor máximo de r (de acordo com a notação da aula) que deverá ser testado em busca de um fator. Em seguida, para cada valor de r de 1 até o valor máximo calculado, o programa deverá imprimir o valor atual de r seguido, na linha abaixo, da tabela do algoritmo de exponenciação modular (conforme Atividade 6.2) usada para testar se o potencial fator primo q calculado a partir do valor atual de r é ou não fator de M(p). Caso seja, o programa deverá imprimir este valor de q, seguido de uma linha com apenas três traços (---). Caso não seja, o programa deverá prosseguir com o próximo valor de r. Caso todos os valores possíveis de r já tenham sido testados e nenhum fator tenha sido encontrado, então M(p) é primo. O programa deverá então imprimir M(p), 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

Saída