Trabalho Individual sobre Raízes Primitivas

Raízes primitivas módulo algum inteiro são muito utilizadas em protocolos criptográficos e em especial em protocolos de acordo de chaves.

a. Descreva o que é uma raíz primitiva e apresente exemplos de seu uso;
b. Desenvolva um programa em Java, C/C++ ou Python para determinar uma raiz primitiva de módulo um número primo *p*. Use o método descrito na seção "Finding primtive roots" que está em em http://en.wikipedia.org/wiki/Primitive_root_modulo_n ou outro método qualquer que seja **mais eficiente** que este. O programa deve trabalhar com primos grandes. Para tal, em Java utilize a classe BigInteger para instanciar e trabalhar com tais números grandes. Python já trabalha com precisão arbitrária. Se você prefere trabalhar em C/C++, considere o uso de uma biblioteca de precisão arbitrária tal como o GMP.
c. Um número primo *p* pode ter muitas raízes primitivas. Sabe-se que uma vez determinada uma das raízes primitivas, todas as outras são facilmente encontradas. Pesquise na literatura e adicione ao seu programa, a determinação de todas as raízes primitivas de um primo *p*, considerando este método. Lembre-se: DADA UMA RAIZ PRIMITIVA é muito fácil e direto obter-se todas as outras raízes.

Entregável: um documento PDF com:

1) Defina raízes primitivas e exemplos de raízes primitivas;
2) O que é o Totiente de Euler de *p*? Qual é a relação, se é que existe, entre o Totiente de Euler de *p* e a quantidade de raízes primitivas de *p*?
3) Determine quantas raízes primitivas tem o primo $p = 1013$.
4) Explique como pode ser obtido de forma eficiente (o mais simples possível), todas as raízes primitivas de um primo *p*, uma vez que se conhece uma das raízes.
5) Sabendo que uma das raízes primitivas de $p = 1013$ é 5, determine todas as outras raízes;
6) Explique o método que você escolheu para encontrar uma raiz primitiva. Mostre um exemplo com valor pequeno de *p*, passo a passo, de como é determinada a raíz primitiva;
7) Sabendo que 5 é uma das raízes primitivas de 23, determine todas as outras raízes;
8) Apresente aplicações (pelo menos duas), com exemplos didáticos, de como usar as raízes primitivas;
9) Insira no relatório (dentro do relatório) o código fonte do programa comentado com exemplos de entrada e saída executadas pelo programa;
10) Gere um primo usando o programa que você desenvolveu anteriormente e depois use este programa para determinar uma raiz primitiva. Mostre o número gerado e a raiz determinada;
11) Tente provar que (também mostre exemplos):

a) Para qualquer primo $p>3$, o produto de suas raízes primitivas é congruente a 1 módulo p;
b) Para qualquer primo p, a soma de suas raízes primitivas é congruente a $\mu(p-1)$, onde μ é a função Möbius.