Álgebra A-UFMG 2015/2
Trabalho Prático- Parte 1
Data de Entrega: Até 28 de novembro de 2015

Programe o método de Fermat para achar fatores de um número de Mersenne. O programa deve ter como entrada um primo p e como saída o menor fator de $M(p) = 2^p - 1$ ou uma mensagem indicando que $M(p)$ é primo. O programa vai consistir, basicamente, de uma implementação do algoritmo da exponenciação para calcular 2^n módulo q onde q é da forma $q = r \cdot 2p + 1$, com $0 \leq r \leq \frac{(2^{p/2}-1)}{2p}$. Se a forma reduzida de 2^p módulo q for 1 então q é fator de $M(p)$; se nenhum tal q for encontrado, então $M(p)$ é primo. Observe que não vale a pena testar se q é primo antes de verificar se é fator de $M(p)$, porque isto só tornaria o programa mais lento. Use este programa para determinar quais os primos p entre 2 e 257 para os quais $M(p)$ é primo. (Ex. 9 Capítulo 9 do Livro texto: Número Inteiros e Criptografia RSA)

Algoritmo da exponenciação:

Entrada: *Inteiros a, e e n, onde $a, n > 0$ e $e \geq 0$.*
Saída: *a forma reduzida de a^e módulo n.*

Etapa 1: Comece com $A = a$, $P = 1$ e $E = e$;

Etapa 2: Se $E = 0$ imprime '$a^e \equiv P(\mod n)$'; senão vai para a Etapa 3;

Etapa 3: Se E for ímpar então atribua a P o valor do resto da divisão de $A \cdot P$ por n e a E o valor $\frac{(E-1)}{2}$ e vá para a Etapa 5, senão vai para Etapa 4;

Etapa 4: Se E for par então atribua a E o valor $\frac{E}{2}$ e vá para a Etapa 5;

Etapa 5: Substitua o valor atual de A pelo resto da divisão de A^2 por n e vá para a Etapa 2.