Universidade Federal de Minas Gerais
Álgebra A– Trabalho Prático 2

Considerações gerais

1. O Trabalho deve ser feito em grupos até de 4 pessoas
2. O Trabalho deve ser entregue até do dia 13/08/2024
3. O Trabalho está formado pela implementação e a documentação.
4. Será aberto um fórum no moodle para responder dúvidas e dar sugestões.

Objetivos O trabalho prático tem como objetivos:

1. Implementar o Algoritmo do crivo quadrático para fatorar número gigantes
2. Na implementação do crivo quadrático será necessário implementar algum algoritmo entre o Algoritmo de Tonelli-Shank ou o Algoritmo de Cipolla para determinar de forma eficiente as soluções de congruências quadrática $x^2 \equiv n \pmod{p}$
3. Também será necessário implementar um algoritmo para solucionar sistemas de equações sobre $\mathbb{Z}_2$. Alguns linguagens já tem algoritmos como Gauss-Jordan implementados, assim só é procurar e adaptar.

Sobre o funcionamento O programa deve ter como entrada dois inteiros $N \gg 0$ a ser fatorado. A saída deve conter a seguinte informação:

1. O limite superior para os primos que serão usando no Crivo, quantos deste primos existem e que podem aparecer na fatoração e o tamanho do vetor de índices j onde ser realizara a procura de tal forma que $f(j) = (j + \lfloor\sqrt{N}\rfloor)^2 - N$ se fatora em primos "pequenos".
2. A saída final deve conter x e y, tais que $x^2 \equiv y^2 \pmod{N}$ e também os números $mdc(x - y, N)$ e $mdc(x + y, N)$

Sobre a implementação

1. Pode ser usada qualquer linguagem de programação desde que seja possível usar precisão aritmética de tamanho arbitrário. Um listado pode ser encontrado na Wikipedia `https://en.wikipedia.org/wiki/List_of_arbitrary-precision_arithmetic_software`
2. Para a eficiência do algoritmo já deve ter em memoria uma lista dos primeiros primos (essa lista pode ser relativamente grande, dependendo do poder computacional).
3. Observe que para a implementação também será necessário implementar um algoritmo solucionar sistemas de equações com entradas em $\mathbb{Z}_2$.

Sobre a documentação A documentação deve conter:

1. Descrição sucinta sobre o desenvolvimento do trabalho.
2. Descrição dos módulos e sua inter-dependência.

3. Descrição do formato de entrada dos dados (a entrada teste sera um arquivo de texto com o número N.
4. Descrição do formato de saída dos dados.
5. Explicação sobre como utilizar o programa.
6. Pesquisar sobre a complexidade de cada um dos algoritmos implementados.
7. Listagem do programa fonte.