Universidade do Minho
Departamento de Matemática e Aplicações

lcc+lmat – 3° ano

Teoria de Números Computacional

teste I — 22 de março de 2018

A duração da prova é de 90 minutos. Justifique todas as suas respostas convenientemente.

As questões 1–3 são resolvidas exclusivamente na folha de prova fornecida, podendo usar o `sagemath` como ferramenta científica.

1. Mostre que se n é um pseudo-primo fraco na base 2, então $N = 2^n - 1$ é um pseudo-primo forte na base 2.

2. Encontre um factor não trivial de $n = 74951$ usando
   (a) a factorização de Fermat;
   (b) o algoritmo de factorização $\rho-$Pollard, com a sucessão pseudo-aleatória dada por $x_0 = 2$ e $f(x) = x^3 + 1$;
   (c) o algoritmo $(p-1)$–Pollard.

3. Considere $n = 25761$.
   (a) Verifique que n não passa o teste de Miller-Rabin de base 2. O que pode concluir sobre a primalidade de n? Construa a respectiva sequência-B.
   (b) Mostre n é um pseudo-primo fraco de base 2.

***

Das questões seguintes, resolva apenas uma delas.

4. sage Suponha que tem à sua disposição uma máquina que permite efectuar operações aritméticas que não exceda $2^{35} - 1$. Implemente uma função que permita somar dois números cujo resultado não seja superior a $(2^{35} - 1)(2^{34} - 1)$. A função deverá ter como argumentos as parcelas e devolver a soma.
   Construa a função num ficheiro de texto com o nome `aXXXXX.sage`. *Escreva, no cabeçalho do ficheiro, o seu nome e curso.*

5. Mostre que $7 \cdot 31 \cdot 73$ é um pseudo-primo absoluto.
   Resolva na folha de prova; não faça uso do `sagemath`.

Cotação:
1:2; 2:(4+4+4); 3:(4+1); 4/5:1