Universidade do Minho
Departamento de Matemática e Aplicações lcc+lmat – 3° ano

Teoria de Números Computacional

teste I (extra) — 20 de abril 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 $\pi(x)$ é assimptótico a $\dfrac{x}{\log x - a}$ para qualquer escolha de a.
   Sugestão: mostre que $\dfrac{\pi(x)}{x} \to_{x\to+\infty} 0$ e recorde que $\pi(x) \sim \dfrac{x}{\log x}$.

2. Encontre um factor não trivial de $n = 132731$ usando
   (a) a factorização de Fermat;
   (b) o algoritmo de factorização $\rho-$Pollard, com a sucessão pseudo-aleatória dada por $x_0 = 3$ e $f(x) = x^2 + 1$;
   (c) o algoritmo $(p-1)$–Pollard.

3. Considere $n = 65281$.
   (a) Verifique que n 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 Um primo p diz-se um *primo de Sophie Germain* se $2p+1$ também for primo. Implemente uma função que encontre todos primos de Sophie Germain menores que um certo argumento dado.
   Construa a função num ficheiro de texto com o nome `aXXXXX.sage`. *Escreva, no cabeçalho do ficheiro, o seu nome e curso.*

5. Numa máquina que opera com números inferiores a 1000, calcule $3243 + 71261$.
   Resolva na folha de prova.

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