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

Teoria de Números Computacional

teste de avaliação — 29 de maio de 2019

A duração da prova é de 120 minutos. Justifique todas as suas respostas convenientemente.

1. Seja $n = 943$. Encontre um divisor não trivial de n usando o algoritmo de factorização de Fermat. Sabe-se que $\sqrt{n} \approx 30.708$. 2 valores

2. Use o algoritmo de factorização ρ-Pollard para encontrar um factor não trivial de $n = 143$, usando a sucessão pseudo-aleatória dada por $x_0 = 2$ e $f(x) = x^2 + 1$. 2 valores

3. Considere o número primo $p = 17$. Sabe-se que $\text{ind}_3 2 = 14$ módulo 17.

   (a) Mostre que 3 é uma raiz primitiva módulo 17, sabendo que $17 \not| (3^8 - 1)$. 2 valores

   (b) Resolva $9^x \equiv 2 \mod 17$. 2 valores

   (c) Usando o sistema de chave pública Elgamal, com chave pública $(p, 3, 2)$, decifre a mensagem interceptada $(2, 5)$. 2 valores

4. Calcule o símbolo de Jacobi $\left(\frac{68}{129}\right)$. 2 valores

5. Sejam p, q primos distintos e $n = pq$. Mostre que a probabilidade de $(x, n) \neq 1$ com $0 \leq x < n$ é $\frac{1}{p} + \frac{1}{q} - \frac{1}{pq}$. 2 valores

6. Mostre, detalhadamente, que qualquer primo ímpar passa o teste de primalidade probabilístico Solovay-Strassen. 2 valores