Universidade do Minho
Departamento de Matemática lcc+lmat – 3º ano

Teoria de Números Computacional

teste de avaliação — 22 de maio de 2021

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

1. Use o algoritmo de factorização de Fermat para factorizar $n = 253$. 3 valores

2. Use o algoritmo ρ-Pollard para factorizar $n = 377$, usando a sequência pseudo-aleatória dada por $f(x) = x^2 - 1$ e $x_0 = 2$ da forma usual.
   Sugestão: sabe-se que $(5, n) = 1 = (190, n)$ e que $(338, n) = 13$. 3 valores

3. Considere $p = 31, r = 3, a = 5$.
   (a) Mostre que r é raiz primitiva de p.
   (b) Usando o parâmetro aleatório $k = 4$, calcule a mensagem cifrada correspondente a $P = 6$ usando o sistema de chave pública ElGamal, com chave pública (p, r, b), onde $b \equiv r^a \mod p$.

   3 valores

4. Verifique que não existe solução para $x^2 \equiv 633 \mod 863$, sabendo que 863 é um número primo. 2 valores

5. Calcule o símbolo de Jacobi $\left(\dfrac{2^5 \cdot 3 \cdot 7^3}{5 \cdot 11 \cdot 17^2}\right)$. 2 valores

6. Considere o primo $p = 19$ e uma sua raiz primitiva $r = 2$. Sabe-se que $\text{ind}_2 5 = 16$ e que $2^{13} \equiv 3 \mod p$. Resolva $15x^7 \equiv 9 \mod p$. 3 valores

7. Seja p um primo ímpar e a tal que $\left(\frac{a}{p}\right) = 1$. Mostre que $\text{ind}_r a$ módulo p é par, onde r é uma raiz primitiva de p. 2 valores

8. Determine os inteiros a para os quais $ax^{11} \equiv 2 \mod 23$ tem solução. 2 valores