Universidade do Minho
Departamento de Matemática

lcc+lmat – 3° ano

Teoria de Números Computacional

exame – época de recurso — 20 de junho de 2023

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

1. Uma chave pública RSA tem os valores $(n, e) = (341, 269)$. Use a factorização de Fermat para obter o texto limpo correspondente ao criptograma interceptado $y = 17$.
   (Sabe-se que $29 \cdot e \equiv 1 \mod 300$) 4 valores

2. Use o algoritmo $(p-1)$-Pollard para factorizar $n = 559$.
   (Sabe-se que $mdc(3, 559) = mdc(63, 559) = 1$.) 2 valores

3. Verifique se $n = 113$ passa o teste de Miller na base 2. O que pode afirmar relativamente à primalidade de n? 2 valores

4. Mostre que 2 é uma raiz primitiva de $p = 37$. Sabendo que $\text{ind}_2(3) = 26$ e que $\text{ind}_2(5) = 23$, resolva $15^x \equiv 9 \mod p$. 2 valores

5. Mostre que não existe solução para a congruência quadrática $x^2 \equiv 118 \mod 263$, sabendo que 263 é um número primo. 2 valores

6. Mostre que 7 é o dígito mais à direita – ou dígito menos significativo – na expansão decimal de $F_n = 2^{2^n} + 1$, para $n \geq 2$. 2 valores

7. Mostre que $5 \cdot 17 \cdot 29$ é um pseudoprimo absoluto (ou número de Carmichael). 3 valores

8. Sabendo a expressão geral para $\left(\frac{2}{p}\right)$, onde p é um primo ímpar, mostre que

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

   onde $n > 2$ é um natural ímpar. 3 valores

*** *Fim* ***