Universidade do Minho
Departamento de Matemática

lcc+lmat – 3° ano

Teoria de Números Computacional

exame – época de recurso — 21 de junho de 2021

A duração da prova é de 180 minutos. Justifique todas as suas respostas convenientemente.

1. Use o algoritmo $(p-1)$–Pollard para encontrar um divisor não trivial de 799. 3 valores

2. Verifique se 137 passa o teste de Miller-Rabin de base 2. O que pode concluir sobre a primalidade de 137? Construa a sequência-B gerada pelo algoritmo de Miller. 3 valores

3. Foi interceptada a mensagem cifrada $c = 40$ numa comunicação que usava uma chave-pública RSA $(119, 5)$.
   Use o algoritmo da divisão por tentativas para calcular $\varphi(119)$ e decifre a mensagem c. 3 valores

4. Verifique se $n = 511$ passa o teste de primalidade de Solovay-Strassen de base 2. 3 valores

5. Indique se existe solução para $x^2 \equiv 7411 \mod 9283$, sabendo que 9283 é primo. 3 valores

6. Suponha que n é tal que $\mathbb{Z}_n^*$ é cíclico, e sejam r uma raiz primitiva módulo n e a e b tais que $(a, n) = (b, n) = 1$. Mostre que $\operatorname{ind}_r(ab) \equiv \operatorname{ind}_r a + \operatorname{ind}_r b \mod \varphi(n)$. 3 valores

7. Mostre que $\varphi(n)$ é par, para todo o natural $n > 2$. 2 valores