Universidade do Minho

Departamento de Matemática e Aplicações — lcc+lmat – 3º ano

Teoria de Números Computacional

teste de avaliação — 27 de maio de 2019

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

1. Verifique se $n = 2^4 \cdot 3 + 1$ passa o teste de Miller na base 2. 2 valores

2. Use o algoritmo $(p-1)$-Pollard para factorizar $n = 77$. 2 valores

3. Considere a chave RSA com parâmetros públicos $(n, e) = (55, 3)$. Calcule $\varphi(n)$. Decifre a mensagem `cripto=8`. (Sabe-se que $3^4 \equiv 1 \mod 40$). 3 valores

4. Considere o primo $p = 19$. Mostre que $r = 2$ é uma raiz primitiva de p. Crie uma chave ElGamal usando os parâmetros p e r. Use a chave pública para cifrar a mensagem `mens=5`. 3 valores

5. Calcule o símbolo de Jacobi $\left(\frac{83}{235}\right)$. 2 valores

6. Mostre que se p é um primo ímpar então
$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1 \mod 4 \\ -1 & \text{se } p \equiv 3 \mod 4 \end{cases}$$
2 valores

7. Suponha que n admite uma raiz primitiva r. Mostre que $\{r^1, r^2, \ldots, r^{\varphi(n)}\}$ é um sistema reduzido de resíduos módulo n. 2 valores