

Teoria de Números Computacional

teste

7 de janeiro de 2026

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

1. Calcule $\varphi(1400)$. 1 valor
2. Sabe-se que $n = 8927$ é o produto de dois primos, e que $\varphi(n) = 8736$. Factorize n . 2 valores
3. Calcule $\left(\frac{131}{897}\right)$. 2 valores
4. Considere o primo $p = 37$. Mostre que $r = 2$ é uma raiz primitiva de p . Verifique se existe solução para

$$6^x \equiv 18 \pmod{p},$$

sabendo que $\text{ind}_r 3 \equiv 26 \pmod{\varphi(p)}$.

3 valores

5. Verifique se $n = 2^4 \cdot 7 + 1$ passa o teste de Miller-Rabin na base 2. Construa a sequência-B. O que pode dizer sobre a primalidade de n ? 2 valores
6. Encontre um factor $n = 1055$ usando o algoritmo ρ -Pollard, usando a sequência pseudo-aleatória dada por $x_0 = 2$ e gerada da forma usual por $f(x) = x^2 + 1$.

Sugestão:

Sabe-se que $434 \equiv 458304 \pmod{n}$, e que 434 e n não têm factores primos em comum.

2 valores

7. Verifique se existe um natural n para o qual

$$657127 \mid (n^2 - 67760),$$

sabendo que 657127 é primo.

2 valores