Universidade do Minho
Departamento de Matemática

lcc+lmat – 3° ano

Teoria de Números Computacional

teste — 5 de junho de 2023

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

1. Seja $n = 3713$. Use o algoritmo de factorização de Fermat para calcular $\varphi(n)$. 2 valores

2. Use o algoritmo ρ-Pollard para factorizar $n = 13603$, usando a sequência pseudo-aleatória dada por $f(x) = x^2 + 1$ e $x_0 = 3$ da forma usual. 2 valores

3. Usando o teste de Miller-Rabin na base 2, averigue se 193 é primo. 2 valores

4. Sabendo que $p = 37$ é primo e que $r = 2$ é uma raiz primitiva de p, e usando o parâmetro aleatório $k = 3$, calcule a mensagem cifrada correspondente a $P = 4$ usando o sistema de chave pública ElGamal, com chave pública $(p, r, 10)$. 2 valores

5. Mostre que 2 é uma raiz primitiva de $p = 29$. Sabendo que $\text{ind}_2(10) = 23$ e que $\text{ind}_2(11) = 25$, resolva $10^x \equiv 22 \mod p$. 2 valores

6. Mostre que $\left(\frac{3131}{3137}\right) = -1$. 2 valores

7. Sejam p, q primos tais que $q \mid (2^p - 1)$. Mostre que $q \equiv 1 \mod p$, e que se p é ímpar então $q \equiv 1 \mod 2p$.
   (Sugestão: Considere $ord_q 2$.) 2 valores

8. Sejam $k = ord_m(a)$ e $s = \prod_{i=1}^{k} a^i$. Mostre que $ord_m(s) = 1$ se k for ímpar, e que $ord_m(s) = 2$ se k for par. Deduza que $\prod_{a \in \mathbb{Z}^*_{p^\ell}} a \equiv -1 \mod p^\ell$, onde p é um primo ímpar e $\ell \geq 1$.
   (Sugestão: recorde que p^ℓ tem raiz primitiva.) 2 valores

*** *Fim* ***