Universidade do Minho
Departamento de Matemática

lcc+lmat – 3° ano

Teoria de Números Computacional

teste — 24 de maio de 2022

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

1. Bob criou uma chave RSA com parâmetros públicos (n, e), com $n = pq$ produto de dois primos ímpares distintos. Suponha que Charlie encontrou $x \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$. Descreva como pode Charlie quebrar a chave. Calcule a probabilidade de Charlie encontrar x nas condições descritas. 2 valores

2. Use o algoritmo $(p-1)$-Pollard para factorizar $n = 77$. 3 valores

3. Considere $p = 127$.

   (a) Usando o teste de primalidade por tentativas, mostre que p é primo. 1 valor

   (b) Mostre que 2 não é uma raiz primitiva de p. 1 valor

   (c) Sabendo que $r = 3$ 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 $(p, r, 10)$. 3 valores

4. Calcule o símbolo de Jacobi $\left(\dfrac{83}{5^3 \cdot 11^2 \cdot 13}\right)$. 3 valores

5. Mostre que 25 é um pseudo-primo de Euler de base 7. 3 valores

6. Mostre que se $\varphi(n) = n - 1$ então n é primo. 2 valores

7. Mostre que se p é um primo tal que $p \equiv 3 \mod 4$ e $\left(\dfrac{a}{p}\right) = 1$ então $a^{\frac{p-3}{4}+1}$ é uma raiz quadrada de a módulo p. 2 valores

*** *Fim* ***