Universidade do Minho
Departamento de Matemática

lcc+lmat – 3° ano

Teoria de Números Computacional

teste — 16 de maio de 2024

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

1. Sabendo que $p = 89$ é primo e que $r = 3$ é uma raiz primitiva de p, Alice usou o sistema criptográfico ElGamal e publicou a chave $(89, 3, 45)$. Bob cifrou uma mensagem, e obteve o criptograma $(\gamma, \delta) = (51, 83)$, que foi interceptado por Eva. Eva sabe que $\mathrm{ind}_3 5 \equiv 70 \mod \varphi(p)$. Mostre como pode Eva obter o texto limpo a partir do criptograma.
   Sugestão: Sabe-se que $1 \equiv 39 \cdot \gamma^{72} \mod p$. 2 valores

2. Sabendo que 997 é primo, mostre que não existe solução para a congruência quadrática $x^2 \equiv 132 \mod 997$. 2 valores

3. Considere o primo $p = 61$ e a sua raiz primitiva $r = 2$. Resolva $6x^{11} \equiv 54 \mod p$, sabendo que $2^6 \equiv 3 \mod p$ e que $11^{-1} \equiv 11 \mod \varphi(p)$. 2 valores

4. Seja $n = 403$. Calcule $\varphi(n)$ usando
   (a) a factorização de Fermat; 2 valores
   (b) o algoritmo $(p-1)$-Pollard.
   Sugestão: Sabe-se que $(63, n) = 1$ e que $(325, n) = 13$. 2 valores

5. Usando o teste de Miller-Rabin na base 2, averigue se 41 é primo. Construa a respetiva sequência-B. 2 valores

6. Seja n o produto de primos ímpares p_i. Mostre que se a é um resíduo quadrático de cada p_i então $\left(\frac{a}{n}\right) = 1$. Mostre que o recíproco não é válido, tomando $a = 2$ e $n = 15$. 2 valores

7. Mostre que $\varphi(n)$ é par, para $n \geq 3$. 2 valores

*** *Fim* ***