Universidade do Minho

Departamento de Matemática e Aplicações — Icc+lmat – 3° ano

Teoria de Números Computacional

teste II — 7 de junho de 2018

A duração da prova é de 90 minutos. Justifique todas as suas respostas convenientemente.

1. Seja p um primo ímpar e a tal que $\left(\frac{a}{p}\right) = 1$. Mostre que $\mathrm{ind}_r a$ módulo p é par, onde r é uma raiz primitiva de p. 4 valores

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

3. Considere o número primo $p = 64439$. 4 valores
   (a) Mostre que 3 não é raiz primitiva módulo p.
   (b) Numa comunicação foi usado o sistema criptográfico ElGamal com a chave pública $(p, 7, 8965)$ para a transmissão de uma certa mensagem que, depois de cifrada, foi interceptada como $(17145, 38180)$. Sabendo que 7 é raiz primitiva módulo p e que $\mathrm{ind}_7 8965 = 101$ módulo p, encontre a mensagem original.

4. Considere a chave pública RSA dada por $(n, e) = (108417259, 32767)$. 4 valores
   (a) Cifre `x=1234`.
   (b) Decifre `y=7279540`, sabendo que 12037 divide n.

*Das seguintes questões, resolva apenas **uma**.*

5. Use o Teste de Lucas-Lehmer para números de Mersenne para verificar se $M_5 = 2^5 - 1$ é um primo de Mersenne. 4 valores

6. Calcule o valor do símbolo de Jacobi $\left(\frac{113}{997}\right)$. 4 valores

7. Verifique se 7813 é um pseudo-primo de Euler de base 5. 4 valores

8. Use o algoritmo de Lucas para mostrar que 71 é primo, usando a base $a = 17$. 4 valores

9. Sejam p, q primos distintos e $n = pq$. Mostre que a probabilidade de $(x, n) \neq 1$ com $0 \leq x < n$ é $\frac{1}{p} + \frac{1}{q} - \frac{1}{pq}$. 4 valores