Universidade do Minho
Departamento de Matemática e Aplicações

lcc+lmat – 3° ano

Teoria de Números Computacional

teste II — 1 de junho de 2018

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

1. Suponha que n é o produto de dois primos distintos. Mostre que factorizar n nos seus primos é equivalente a calcular $\phi(n)$. 4 valores

2. Mostre que se r é uma raiz primitiva módulo de m e $(x, m) = (y, m) = 1$ então

$$\text{ind}_r(xy) \equiv \text{ind}_r x + \text{ind}_r y \mod \phi(m).$$

4 valores

3. Considere o número primo $p = 26339$. 4 valores

   (a) Mostre que 3 não é raiz primitiva módulo p.

   (b) Numa comunicação foi usado o sistema criprográfico ElGamal com a chave pública $(p, 2, 8967)$ para a transmissão de uma certa mensagem que, depois de cifrada, foi interceptada como $(19113, 12170)$. Sabendo que 2 é raiz primitiva módulo p e que $\text{ind}_2 8967 = 101$ módulo p, encontre a mensagem original.

4. Considere a chave pública RSA dada por $(n, e) = (120154049, 32767)$. 4 valores

   (a) Cifre `x=1234`.

   (b) Decifre `y=1221249`, sabendo que 10007 divide n.

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

5. Use o Teste de Lucas-Lehmer para números de Mersenne para verificar se $M_7 = 2^7 - 1$ é um primo de Mersenne. 4 valores

6. Calcule o valor do símbolo de Jacobi $\left(\dfrac{83}{235}\right)$. 4 valores

7. Verifique se 8401 é um pseudo-primo de Euler de base 3. 4 valores

8. Use o algoritmo de Lucas para mostrar que $2^2 \cdot 7 + 1$ é primo. 4 valores