Universidade do Minho
Departamento de Matemática e Aplicações Icc+lmat – 3° ano

Teoria de Números Computacional

exame de recurso — 21 de junho de 2019

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

Parte I

1. Sabendo que 101 é um número primo, mostre que não existem soluções para a congruência $x^2 \equiv 90 \mod 101$. 3 valores

2. Verifique se $n = 727$ passa o teste de primalidade de Solovay-Strassen de base 3. O que pode dizer sobre a primalidade de n?
   Sugestão: Sabe-se que $2^{60} \equiv 350 \mod 727$. 3 valores

3. Enuncie o teste probabilístico de primalidade de Miller-Rabin. Mostre que 57 não passa o teste de Miller-Rabin de base 2.
   [*Sugestão*: $2^{14} \not\equiv -1 \mod 57$ e $2^{28} \not\equiv -1 \mod 57$.] 3 valores

4. Considere o produto de dois primos distintos $n = 161$. Resolva **apenas uma** das alíneas seguintes:

   (a) Use a factorização de Fermat para encontrar p primo tal que $p|n$. 3 valores

   (b) Use o algoritmo $(p-1)$–Pollard para encontrar um divisor não trivial de n.
   [*Sugestão*: Sabe-se que $(63, n) = 7$.] 3 valores

   (c) Factorize 143 usando o algoritmo ρ–Pollard, usando a sequência pseudo-aleatória dada por $x_0 = 2$ e gerada da forma usual por $f(x) = x^2 + 1$.
   [*Sugestão*: Sabe-se que $(21, n) = 1$ e que $(132, 143) = 11$.] 3 valores

5. Suponha que n é o produto de dois primos distintos. Mostre que factorizar n nos seus primos é equivalente a calcular $\varphi(n)$. 2 valores

6. Mostre que se n é um pseudoprimo fraco de base 2 então $N = 2^n - 1$ é um pseudoprimo forte de base 2. 2 valores

***

Não resolva as questões seguintes se pretender manter a sua classificação do Trabalho Prático. Nesse caso, obter 8,0 valores na Parte I é condição necessária para ter aprovação na UC

***

Parte II

7. Considere o número primo $p = 37$. Numa comunicação foi usado o esquema Elgamal com a chave pública $(p, 2, 28)$ para a transmissão de uma certa mensagem que, depois de cifrada, foi interceptada como $(21, 8)$. Sabendo que 2 é raiz primitiva módulo p e que $\text{ind}_2 28 = 34$ módulo p, encontre a mensagem original. 2 valores

8. Considere a chave RSA com parâmetros públicos $(n, e) = (55, 3)$. Calcule $\varphi(n)$. Decifre a mensagem `cripto=8`. (Sabe-se que $3^4 \equiv 1 \mod 40$). 2 valores