Universidade do Minho
Departamento de Matemática

lcc+lmat – 3° ano

Teoria de Números Computacional

exame — 15 de junho de 2022

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

1. Considere a chave pública RSA dada por $(n, e) = (120154049, 32767)$. Decifre `y=1221249`, sabendo que 10007 divide n. 2 valores

2. Encontre um factor não trivial de $n = 132731$ usando

   (a) a factorização de Fermat; 2 valores

   (b) o algoritmo de factorização $\rho-$Pollard, com a sucessão pseudo-aleatória dada por $x_0 = 3$ e $f(x) = x^2 + 1$. 2 valores

3. Considere $n = 65281$. Verifique se n passa o teste de Miller-Rabin de base 2. O que pode concluir sobre a primalidade de n? 2 valores

4. Considere o número primo $p = 31$. Numa comunicação foi usado o esquema ElGamal com a chave pública $(p, 3, 7)$ para a transmissão de uma certa mensagem que, depois de cifrada, foi interceptada como $(9, 19)$. Sabendo que 3 é raiz primitiva de p e que $\text{ind}_3 7 = 28$, encontre a mensagem original. 2 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 p é um primo ímpar, com $p \neq 3$, então

$$\left(\frac{3}{p}\right) = 1 \text{ se e só se } p \equiv \pm 1 \mod 12.$$

2 valores

Parte prática

Resolva as questões seguintes apenas se não pretender manter a classificação obtida nos trabalhos e mini-testes.

1. Encontre o menor pseudoprimo de Euler de bases 2, 3 e 5, simultaneamente.

2. Suponha que tem à sua disposição uma máquina que permite efectuar operações aritméticas que não excedam 2^{35}. Calcule

$$1237940039285 + 24758800785707605.$$