Universidade do Minho
Departamento de Matemática

L.E.M., L.M.C.C. – 4° ano
Mat. (Esp. Ensino), L.C.C. – 3° ano

Teoria de Números Computacional

exame - 1^a chamada — 12 de junho de 2007

A duração do exame é de 2 (duas) horas.

O exame consiste em duas partes. Resolva-as em folhas de exame distintas. Caso pretenda manter a sua classificação referente aos trabalhos práticos, **não** resolva a parte II, caso contrário a sua classificação anterior perderá a validade. Entregue **ambas** as folhas de exame, ainda que vazias.

Justifique todas as suas respostas convenientemente.

É permitida a utilização de máquinas de calcular

Parte I

1. Para $n > 1$, mostre que $n \mid \phi(2^n - 1)$.
   [Sugestão: Mostre, em primeiro lugar, que $\mathrm{ord}_{2^n-1} 2 = n$.]

2. (a) Mostre que se p é um primo ímpar então
$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1 \mod 4 \\ -1 & \text{se } p \equiv 3 \mod 4 \end{cases}$$
   (b) Demonstre o critério de Euler: se $p \neq 2$ é primo e $p \nmid a$ então $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.
   (c) Use as alíneas anteriores para calcular o símbolo de Jabobi $\left(\frac{-38}{39}\right)$.

3. Sejam $m, k \in \mathbb{N}$ e r uma raiz primitiva de m. Mostre que se $(a, m) = 1$ então
$$\mathrm{ind}_r a^k \equiv k \cdot \mathrm{ind}_r a \mod \phi(m).$$

4. Considere $p = 17, r = 3, a = 5$.
   (a) Mostre que r é raiz primitiva de p.
   (b) Usando o parâmetro aleatório $k = 4$, calcule a mensagem cifrada correspondente a $P = 12$ usando o sistema de chave pública ElGamal, com chave pública (p, r, b), onde $b \equiv r^a \mod p$.

Parte II

5. Uma certa chave pública RSA é $(n, e) = (1520273, 575843)$, onde n é o produto de dois primos distintos e e é o expoente de cifração. Usando a factorização de Fermat, calcule $\phi(n)$. Se a mensagem 1218147 for interceptada por uma terceira pessoa, indique a forma como esta poderá obter a mensagem original.

6. Use o algoritmo $(p-1)$–Pollard para encontrar um divisor não trivial de 689.

7. Enuncie o teste probabilístico de primalidade de Miller-Rabin. Mostre que 2047 passa o teste de Miller de base 2.
   [Sugestão: Repare que $2^{1023} = \left(2^{11}\right)^9 3 = (2048)^9 3$.]