Universidade do Minho — L.E.M., L.M.C.C. – 4° ano
Departamento de Matemática — Mat. (Esp. Ensino), L.C.C. – 3° ano

Teoria de Números Computacional

exame - 2^a chamada — 28 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. Sejam p, q primos distintos e $n = pq$. Se $1 \leq x < n$, mostre que a probabilidade de $(x, n) \neq 1$ é $\frac{1}{p} + \frac{1}{q} - \frac{1}{pq}$.

2. Sejam p um primo ímpar, e a, b duas raízes primitivas módulo p. Mostre que ab não é raiz primitiva módulo p.

3. Calcule o símbolo de Jacobi $\left(\frac{7}{177}\right)$.
   [Sugestão: $177 = 3 \cdot 59$ e use a Lei da Reciprocidade Quadrática.]

4. Sejam $p \neq 2$ um primo e r uma raiz primitiva de p. Mostre que se $p \nmid a$ então $\text{ind}_r a$ é par se e só se a é um resíduo quadrático módulo p.

5. Mostre que $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$, onde p é um primo e α é um natural.

6. Considere $p = 19, r = 2, a = 5$.
   (a) Mostre que r é raiz primitiva de p.
   (b) Usando o parâmetro aleatório $k = 4$, calcule a mensagem cifrada correspondente a $P = 6$ usando o sistema de chave pública ElGamal, com chave pública (p, r, b), onde $b \equiv r^a \mod p$.

Parte II

7. Sabendo que $2^{693} \equiv 512 \mod 1387$ e que $1386 = 2 \cdot 693$, mostre que 1387 não passa o teste de Miller de base 2. O que pode concluir sobre a primalidade de 1387?

8. Use o Algoritmo de factorização ρ-Pollard para encontrar um factor não trivial de 8051, usando a sucessão pseudo-aleatória dada por $x_0 = 2$ e $f(x) = x^2 + 1$.
   [Sugestão: $(21, 8051) = (7448, 8051) = 1$ e $(194, 8051) = 97$.]

9. Use o Teste de Lucas-Lehmer para números de Mersenne para mostrar que $M_5 = 2^5 - 1$ é um primo de Mersenne.

Cotação:
cada questão/alínea: 2 valores