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 - época de recurso — 25 de julho 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

Das questões seguintes, resolva *apenas* 7.

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

2. Enuncie e demonstre o Critério de Euler.

3. Mostre que se o primo ímpar p não divide a nem b então
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

4. Mostre que 5 é raiz primitiva de 23.

5. Considere $p = 23, r = 5, a = 3$. Usando o parâmetro aleatório $k = 3$, e sabendo que r é raiz primitiva de p, calcule a mensagem cifrada correspondente a $P = 4$ usando o sistema de chave pública ElGamal, com chave pública (p, r, b), onde $b \equiv r^a \mod p$.

6. Demonstre a validade do teste de primalidade de Lucas-Lehmer: se $n \in \mathbb{N}$ e existir $x \in \mathbb{N}$ para o qual $x^{n-1} \equiv 1 \mod n$ e $x^{\frac{n-1}{q}} \not\equiv 1 \mod n$ para todo o factor primo q de $n-1$, então n é primo. A x chamamos "testemunha" (testemunha a primalidade de n).
[*Sugestão:* deduza, da hipótese, que $\mathrm{ord}_n x = n-1$ e que $\phi(n) = n-1$.]

7. Use o teste de Lucas-Lehmer para mostrar que 19 é primo. Para tal, use 2 como "testemunha".

8. Calcule $\phi(25)$ e faça uso do Teorema de Euler para mostrar que 25 é um pseudo-primo fraco de base 7.

9. Mostre que 25 é um pseudo-primo de Euler de base 7.

Cotação:

cada questão: 2 valores