Universidade do Minho

Departamento de Matemática — Lic. Matemática, Lic. Ciências da Computação – 3° ano

Teoria de Números Computacional

teste II – MAT / teste final – CC — 18 junho '08

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

Justifique todas as suas respostas convenientemente.

É permitida a utilização de máquinas de calcular.

1. Considere o número primo $p = 17$.

   (a) Indique, justificando, um sistema reduzido de resíduos módulo 17. 1 valor

   (b) Mostre que 3 é uma raiz primitiva módulo 17, sabendo que $17 \not| (3^8 - 1)$. 1 valor

   (c) Sabendo $\text{ind}_3 2 = 14$ módulo 17, resolva $9^x \equiv 2 \mod 17$. 3 valores

   (d) Usando o sistema de chave pública Elgamal, com chave pública $(p, 3, 2)$, 3 valores

      i. calcule a mensagem cifrada correspondente a $x = 4$, usando o parâmetro aleatório $k = 3$;

      ii. decifre a mensagem interceptada $(2, 5)$.

2. (a) Mostre que se p é um primo ímpar então

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1 \mod 4 \\ -1 & \text{se } p \equiv 3 \mod 4 \end{cases}$$

   3 valores

   (b) Verifique se existe solução para a congruência $x^2 \equiv 70 \mod 73$. 3 valores

3. (**Apenas** para CC)

   (a) Para $n = 561 = 3 \cdot 11 \cdot 17$, mostre que n é um pseudoprimo absoluto. 2.5 valores

   (b) Mostre que $n = 25$ não passa o teste de Miller-Rabin de base 2. 2.5 valores

***

Das questões seguintes, resolva 2 (MAT) ou 3 (CC) delas:

4. Dada uma certa chave pública RSA (n, e) soube-se o valor de $\phi(n)$. Mostre, detalhadamente, como se pode obter o texto original x tendo-se interceptado o texto cifrado y. 3 valores

5. Calcule o símbolo de Jacobi $\left(\frac{21}{235}\right)$. 3 valores

6. Mostre que se r é uma raiz primitiva módulo de m e $(x, m) = (y, m) = 1$ então $\text{ind}_r(xy) \equiv \text{ind}_r x + \text{ind}_r y \mod \phi(m)$. 3 valores

7. Sejam p, q primos distintos e $n = pq$. Mostre que a probabilidade de $(x, n) \neq 1$ com $0 \leq x < n$ é $\frac{1}{p} + \frac{1}{q} - \frac{1}{pq}$. 3 valores

8. Use o algoritmo de Lucas-Lehmer para mostrar que $2^2 \cdot 7 + 1$ é primo, sabendo que $2^{14} \not\equiv 1 \mod 29$ e $2^{28} \equiv 1 \mod 29$. 3 valores

9. Mostre que 25 é um pseudo-primo de Euler de base 7, sabendo que $7^6 \equiv -1 \mod 25$. 3 valores

10. Mostre que se n é um pseudoprimo fraco de base 2 então $N = 2^n - 1$ é um pseudoprimo forte de base 2. 3 valores

11. Descreva o algoritmo de Lucas-Lehmer para primos de Mersenne. 3 valores