Universidade do Minho

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

Teoria de Números Computacional

exame — 11 julho '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 $p = 31$.

   (a) Mostre que 2 não é raiz primitiva módulo p. 2 valores

   (b) Numa comunicação foi usado o esquema Elgamal com a chave pública $(31, 3, 7)$ para a transmissão de uma certa mensagem que, depois de cifrada, foi interceptada como $(9, 19)$. Sabendo que 3 é raiz primitiva módulo 31 e que $\text{ind}_3 7 = 28$ módulo p, encontre a mensagem original. 2 valores

2. Use o algoritmo $(p-1)$–Pollard para encontrar um divisor não trivial de 91. 2 valores

3. Considere o produto de dois primos distintos $n = 2183$.

   (a) Use a factorização de Fermat para encontrar p primo tal que $p|n$. 2 valores

   (b) Factorize n usando o algoritmo ρ–Pollard, usando a sequência pseudo-aleatória dada por $x_0 = 2$ e gerada da forma usual por $f(x) = x^2 + 1$.
   [*Sugestão*: Sabe-se que $(21, n) = 1 = (2057, n)$ e que $(814, n) = 37$.] 2 valores

4. Mostre, detalhadamente, que qualquer primo ímpar passa o teste de primalidade probabilístico Solovay-Strassen. 2 valores

5. Suponha que n é o produto de dois primos distintos. Mostre que factorizar n nos seus primos é equivalente a calcular $\phi(n)$. 2 valores

***

Das questões seguintes, resolva apenas 3 delas:

6. Mostre, detalhadamente, que qualquer primo ímpar passa o teste de primalidade probabilístico Miller-Rabin. 2 valores

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

8. 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 $\text{ord}_n x = n-1$ e que $\phi(n) = n-1$.] 2 valores

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

10. Sabendo que 101 é um número primo, mostre que não existem soluções para a congruência $x^2 \equiv 90 \mod 101$. 2 valores

11. Enuncie o teste probabilístico de primalidade de Miller-Rabin. Mostre que 57 não passa o teste de Miller-Rabin de base 2.
    [*Sugestão*: $2^{14} \not\equiv -1 \mod 57$ e $2^{28} \not\equiv -1 \mod 57$.] 2 valores