Universidade do Minho
Departamento de Matemática

Lic. Ciências da Computação – 3° ano

Teoria de Números Computacional

exame — 10 julho '09

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

Justifique todas as suas respostas convenientemente.

Esta prova é de consulta e é permitida a utilização de máquinas de calcular.

1. Mostre, detalhadamente, que se p é primo então $\sqrt{p}$ é um irracional.
2. Mostre que 7 é o último dígito (na expansão decimal) de F_n, para $n \geq 2$.
3. Mostre que, para $n \geq 2$, são válidas as desigualdades $\frac{1}{2}\sqrt{n} \leq \phi(n) \leq n - 1$.
   Sugestão: Mostre que, para qualquer real $x \geq 3$, se tem $x - 1 \geq \sqrt{x}$.

***

Das questões seguintes, resolva apenas 7 delas:

4. Use o teste de Lucas-Lehmer para verificar se M_7 é um primo de Mersenne.
5. Verifique se existe $n \in \mathbb{N}$ para o qual $n^2 \equiv 1221 \mod 7621$.
6. Mostre que $7 \cdot 31 \cdot 73$ é um pseudoprimo absoluto.
7. Verifique se $n = 2^5 \cdot 21 + 1$ passa o teste de Miller-Rabin de base 2. Construa a sequência-B. O que pode dizer sobre a primalidade de n?
   Sugestão: Sabe-se que $n \mid (2^{21} - 84)$.
8. Verifique se $n = 727$ passa o teste de primalidade de Solovay-Strassen de base 3. O que pode dizer sobre a primalidade de n?
   Sugestão: Sabe-se que $2^{60} \equiv 350 \mod 727$.
9. Encontre um factor $n = 1055$ 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 434 e n não têm factores primos em comum.
10. Mostre que 2 é uma raiz primitiva de 37. Use o algoritmo de Shanks para resolver a congruência $2^x \equiv 22 \mod 37$.
11. Numa comunicação foi usado o esquema Elgamal com a chave pública $(37, 2, 22)$ para a transmissão de uma certa mensagem que, depois de cifrada, foi interceptada como $(2, 29)$. Sabendo que $\text{ind}_2 22 = 31$ módulo 37, encontre a mensagem original.
12. Sabendo que $(e, n) = (411, 667)$ é uma chave pública RSA, use a factorização de Fermat para decifrar a mensagem interceptada $y = 375$.
    Sugestão: $3 \cdot 411 \equiv 1 \mod 616$

Cotação:
1–12: 2.