Teoria de Números Computacional

folha iii — 2° semestre, 2006/2007

1. Pretende-se determinar $\dfrac{\pi(x)}{\frac{x}{\log x}}$, para alguns valores de x.
   (a) Escreva uma função que tenha como argumento n e devolva $\pi(n)$, $\frac{x}{\log x}$ e $\dfrac{\pi(x)}{\frac{x}{\log x}}$.
   (b) Use o comando `intnum` para aproximar $\pi(x)$ à custa de $\int_2^x \frac{dt}{\log t}$.
   (c) Use o comando `ploth` para esboçar os gráficos de $\pi(x), Li(x)$ e de $\frac{x}{\log x}$.
2. Use a factorização de Fermat para encontrar uma factorização de
   (a) 143
   (b) 43
   (c) 2279
   (d) 11413
   (e) 8051
   (f) 11021
   (g) 73
   (h) 46009
   (i) 3200399
   (j) 24681023
3. Implemente uma função que factorize um número segundo o método de Fermat.
4. Escreva uma função que resolva a equação diofantina $ax + by = c$.
5. Mostre que
   (a) se a é um inteiro par então $a^2 \equiv 0 \mod 4$;
   (b) se a é um inteiro ímpar então $a^2 \equiv 1 \mod 4$.
6. Mostre que se a é um inteiro ímpar então $a^2 \equiv 1 \mod 8$.
7. O que pode concluir se $a^2 \equiv b^2 \mod p$, onde $a, b \in \mathbb{Z}$ e p é primo?
8. Encontre as soluções de:
   (a) $123456789x \equiv 9876543210 \mod 10000000001$
   (b) $333333333x \equiv 87543211376 \mod 967454302211$

(c) $734342499999x \equiv 1 \mod 1533331$

(d) $499999x \equiv 1 \mod 1533331$

(e) $1000001x \equiv 1 \mod 1533331$

9. Use ρ-Pollard, com $x_0 = 2$ e $f(x) = x^2 + 1$ para encontrar a factorização de

   (a) 133

   (b) 1189

   (c) 1927

   (d) 8131

   (e) 36287

   (f) 48227

10. Use ρ-Pollard para factorizar 1387, fazendo uso de

   (a) $x_0 = 2; f(x) = x^2 + 1$

   (b) $x_0 = 3; f(x) = x^2 + 1$

   (c) $x_0 = 2; f(x) = x^2 - 1$

   (d) $x_0 = 2; f(x) = x^3 + x + 1$