Universidade do Minho
Departamento de Matemática L.C.C. – 3° ano

Teoria de Números Computacional

folha iii — 2° semestre, 2008/2009

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 $\pi(n)$, $\frac{x}{\log x - 1}$ e $\dfrac{\pi(x)}{\frac{x}{\log x-1}}$.

   (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. Mostre que se $n \equiv 2 \mod 4$ então n não se pode escrever como diferença de quadrados.

4. Implemente uma função que factorize um número segundo o método de Fermat.

5. Verifique a igualdade de Aurifeuille:

$$2^{4n+2} + 1 = \left(2^{2n+1} - 2^{n+1} + 1\right)\left(2^{2n+1} + 2^{n+1} + 1\right).$$

   Use-a para obter uma factorização não trivial de $2^{58} + 1$.

6. Escreva uma função que resolva a equação diofantina $ax + by = c$.

7. Mostre que

   (a) se a é um inteiro par então $a^2 \equiv 0 \mod 4$;

   (b) se a é um inteiro ímpar então $a^2 \equiv 1 \mod 4$.

8. Mostre que se a é um inteiro ímpar então $a^2 \equiv 1 \mod 8$.

9. O que pode concluir se $a^2 \equiv b^2 \mod p$, onde $a, b \in \mathbb{Z}$ e p é primo?

10. 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) $1000001x \equiv 1 \mod 1533331$

11. Mostre que $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, enquanto anéis, para $(m, n) = 1$.
    Sugestão: considere o homomorfismo $\psi([a]_{mn}) = ([a]_m, [a]_n)$.

12. Numa máquina que opera com números inferiores a 100, calcule

    (a) $323 + 1261$

    (b) $123655 + 410231$

    (c) 124×201

13. Numa máquina que opera com números inferiores a 1000, calcule

    (a) $3243 + 71261$

    (b) $4009143 + 2107002$

    (c) 1003×4101

14. Sejam $a, b \in \mathbb{N}$ com $a > b$. Mostre que

    (a) se r é o resto da divisão de a por b então $2^r - 1$ é o resto da divisão de $2^a - 1$ por $2^b - 1$. Como sugestão, observe que

    $$2^{bq+r} - 1 = \left(2^b - 1\right)\left(2^{b(q-1)+r} + \cdots + 2^{b+r} + 2^r\right) + (2^r - 1)\,.$$

    (b) $\left(2^a - 1, 2^b - 1\right) = 2^{(a,b)} - 1$.

    (c) $\left(2^a - 1, 2^b - 1\right) = 1$ se e só se $(a, b) = 1$.

15. Suponha que tem à sua disposição uma máquina que permite efectuar operações aritméticas que não excedam 2^{35}, e que pretende calcular o produto de 12379400392853802748991242 25 por 2475880078570760549798248453. Mostre como tal se pode efectuar.
    Sugestão: defina `m1=2^35-1; m2=2^34-1; m3=2^33-1; m4=2^31-1;m5=2^29-1;m6=2^23-1;` e `M=m1*m2*m3*m4*m5*m6`, e considere o Teorema Chinês dos Restos.

16. 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

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