Unidade de Ensino de Matemática Aplicada e Análise Numérica
Departamento de Matemática/Instituto Superior Técnico

Matemática Experimental (LMAC) – 1º Semestre de 2020/2021

Trabalho Computacional

1. Seja $n \in \mathbb{N}$ um inteiro ímpar (candidato para ser primo) que tenha passado o teste de pseudoprimalidade na base b, i.e.

$$b^{n-1} \equiv 1 \pmod{n}\,, \qquad \mathrm{mdc}(b,n) = 1\,.$$

Escreva $n = 2^\alpha\, t + 1$ em que $\alpha, t \in \mathbb{N}$ e t é ímpar.

a) Verifique que

$$b^{n-1} - 1 = (b^t - 1)\,(b^t + 1)\,(b^{2t} + 1)\,(b^{4t} + 1)\cdots(b^{2^{\alpha-1}t} + 1)\,. \tag{1}$$

b) Um inteiro ímpar diz-se *pseudoprimo forte na base b* se dividir um e um só dos fatores do lado direito na equação (1).

Implementente, em linguagem `Mathematica`, o seguinte pseudocódigo para testar a pseudoprimalidade forte (na base b) de um inteiro n:

1. `Input`: $n, b \in \mathbb{N}, n \geq 3$ ímpar, $b \geq 2$, tais que `mdc`$(b,n) = 1$.
2. $t \leftarrow n-1$; $a \leftarrow 0$;
3. `While` t é par `do` $t \leftarrow t/2$; $a \leftarrow a+1$;
4. $x \leftarrow$ `Powermod`(b,t,n);
5. `If` $x = 1$ `or` $n-1$ `then` *teste* $\leftarrow$ `True else`
  a) `For` $i = 1$ `to` $a-1$ `do`
    $x \leftarrow (x * x) \bmod n$;
    `If` $x = n-1$ `then` (*teste* $\leftarrow$ `True`; `Return`)
  b) *teste* $\leftarrow$ `False`

c) Determine o primeiro pseudoprimo forte na base 2. Determine o número de pseudoprimos e o número de pseudoprimos fortes na base 2 até 10^6. Idem para 10^9.

d) Determine o número de pseudoprimos $\leq 25 \cdot 10^9$ que passam o teste de pseudoprimalidade nas bases $2, 3, 5$ e 7. Verifique que apenas um número composto passa o teste de pseudoprimalidade forte nas bases $2, 3, 5$ e 7. Qual?

e) Determine os pseudoprimos na base 2 entre 10^{100} (o `googol`) e $10^{100} + 1000$. Escreva um código que devolva os pseudoprimos na forma $n = 10^{100} + x$.

f) Um *número de Carmichael* é um número composto n, ímpar, que passa o teste de pseudoprimalidade na base b para cada $b, 1 < b < n$. Determine todos os números de Carmichael inferiores a 10 000. Determine os números de Carmichael compostos de 4 factores primos.

g) Confirme que o número composto n é um número de Carmichael se e só se não for divisível por um quadrado perfeito (diferente de 1) e todos os seus divisores primos p são tais que $(p-1)|(n-1)$.

2. Um natural b diz-se *resíduo quadrático módulo* p se $\mathrm{mdc}(b,p)=1$ e se existir um inteiro t tal que $b \equiv t^2 \pmod p$. O critério de Euler afirma que b é resíduo quadrático módulo p se e só se $b^{(p-1)/2} \equiv 1 \pmod p$.

a) Escreva um programa `Mathematica` que lhe permita pronunciar sobre a veracidade ou falsidade da afirmação:

Se b for composto então $b = c\,d$ é resíduo quadrático módulo p se e só se ou c e d são ambos resíduos quadráticos ou nenhum dos dois é resíduo quadrático módulo p.

b) Dados um primo `b` e um inteiro `nmax` ≥ 3, escreva um programa `Mathematica` para produzir uma lista de primos ímpares não superiores a `nmax` para os quais `b` é resíduo quadrático. Teste o seu programa para `nmax` $= 100$ e `b` $= 2, 3, 5, 7, 11, 13, 17$, apresentando os resultados numa tabela.

c) Desenvolva um código `Mathematica` que lhe permita conferir o seguinte resultado: Dados dois primos distintos $p, q \geq 3$, p é resíduo quadrático módulo q se e só se q é resíduo quadrático módulo p excepto quando p e q são ambos congruentes com 3 módulo 4 em que caso p é resíduo quadrático módulo q se e só se q é resíduo não quadrático módulo p.

d) Seja $p \geq 3$ um primo. Aplique o código da alínea **c)** para confirmar que

- **i.** 3 é resíduo quadrático módulo p se e só se $p \equiv \pm 1 \pmod{12}$;
- **ii.** 5 é resíduo quadrático módulo p se e só se $p \equiv \pm 1 \pmod 5$;
- **iii.** 7 é resíduo quadrático módulo p se e só se $p \equiv \pm 1, \pm 3$ ou $\pm 9 \pmod{28}$;
- **iv.** 13 é resíduo quadrático módulo p se e só se $p \equiv \pm 1, \pm 3$ ou $\pm 4 \pmod{13}$.

e) Os números de Fermat F_k definem-se por

$$F_k = 2^{2^k} + 1, \qquad k = 0, 1, \ldots .$$

Prove que 3 é resíduo não quadrático módulo número de Fermat primo.

(<u>Sugestão:</u> Mostre que $F_k \equiv 5 \pmod{12}$).

f)[Teste de Pépin] Confirme que o número de Fermat F_k é primo se e só se

$$3^{(F_k-1)/2} \equiv -1 \pmod{F_k}\,.$$

g) Escreva um programa `Mathematica` que receba $a, b, c \in \mathbb{Z}$ e p, um primo, e devolva as soluções (se existirem) da equação

$$a\,x^2 + b\,x + c \equiv 0 \pmod p$$

Considere separadamente os seguintes casos

- **i.** $p = 2$. Note-se que $x^2 \equiv x \pmod 2$;
- **ii.** $p \mid a$;
- **iii.** $p > 2$ e $p \nmid a$. Neste caso o problema pode ser escrito na forma equivalente

$$(x + 2^{-1}a^{-1}b)^2 \equiv 4^{-1}a^{-2}b^2 - a^{-1}c \pmod p\,.$$

Teste o seu programa escolhendo diferentes valores para a, b, c e p.

3. Sejam (m, n) pares de inteiros tais que $80 \leq m, n \leq 95$ e considere um grafo orientado em que os vértices são os números entre 80 e 95 e cada aresta é um par (m, n) se mn for primo. Por exemplo, existe uma aresta entre 90 e 91 visto que 9091 é primo.

a) Utilize o comando `GraphPlot` para desenhar este grafo. O aspecto do seu grafo devia ser como no exemplo da Figura 1.

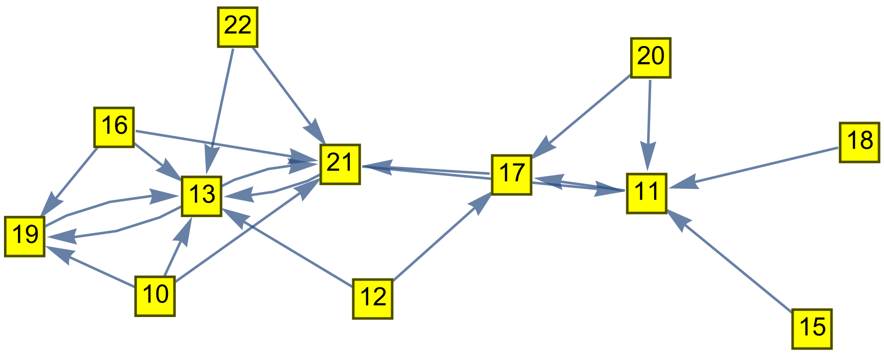

Figura 1: Um grafo orientado.

b) Recorra ao comando `Manipulate` para poder observar, de forma interativa, como o grafo se altera quando $m, n \in [10j, 10j + 15]$, com $j = 1, 2, \ldots, 10$.

4. Um inteiro positivo n diz-se *número estranho* se a soma dos seus divisores próprios é maior do que o número n, mas a soma de nenhum subconjunto desses divisores é igual a n. Determine os primeiros quatro números estranhos. Verifique que todos os números da forma $70\,p$ onde $p \geq 149$ é primo, são números estranhos.

5. Seja N um número natural com número par de dígitos n tal que N pode ser fatorizado em dois naturais x e y, cada um com $n/2$ dígitos e não ambos a terminar em zero, e tais que os dígitos de x e y são precisamente os dígitos de N, por exemplo $N = 1260 = 21 \times 60$. Determine os números desta forma com $n = 2$ e $n = 4$ dígitos. Quantos números destes existem com 6 e 8 dígitos?

6. Um inteiro P_n gerado pela fórmula de recorrência

$$P_n = P_{n-2} + P_{n-3}\,, \quad n = 3, 4, \ldots\,, \qquad P_0 = 3\,,\ P_1 = 0\,,\ P_2 = 2\,,$$

diz-se *número de Perrin.*

a) Confirme que os números de Perrin podem ser calculados explicitamente pela fórmula

$$P_n = r^n + q^n + s^n\,,$$

onde r, q e s são as raízes distintas da equação carcterística $x^3 - x - 1 = 0$; r é real e q, s são complexos conjugados.

b) Verifique que

$$\begin{pmatrix} P_n \\ P_{n+1} \\ P_{n+2} \end{pmatrix} = A^n \begin{pmatrix} 3 \\ 0 \\ 2 \end{pmatrix}, \qquad \text{onde} \quad A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

c) Ao número r chama-se *número plástico*. Verifique que

$$r = \sqrt[3]{1 + \sqrt[3]{1 + \sqrt[3]{1 + \ldots}}}.$$

d) Mostre que

$$\lim_{n \to \infty} P_n = r^n \, .$$

e) Confirme que $p \mid P_p$ se p for primo.

f) Um número composto n que divide P_n diz-se *pseudoprimo de Perrin*. Determine os primeiros 10 pseudoprimos de Perrin.

7. O teorema de Zeckendorf afirma que qualquer $n \in \mathbb{N}$ pode ser representado, de forma única, como soma de números de Fibonacci não consecutivos. Mais precisamente

$$n = F_{k_1} + F_{k_2} + \cdots + F_{k_r} \, , \quad k_j \geq k_{j+1} + 2, j = 1, \ldots, k_r, \quad k_r \geq 2 \, ,$$

onde F_{k_j} é o k_j-ésimo número de Fibonacci. Por exemplo, $45 = 34 + 8 + 3 = F_9 + F_6 + F_4$.

a) Defina uma função `Mathematica` que receba um inteiro positivo n e devolva a representação de Zeckendorf de n. A sua função deve retornar a lista de números de Fibonacci não consecutivos F_{k_j} tais que $n = F_{k_1} + F_{k_2} + \cdots + F_{k_r}$ e a representação binária de n (na base de números de Fibonacci), i.e. os coeficientes d_j tais que

$$n = \sum_{j=0}^{k_1} d_j F_j \, , \qquad n = (d_{k_1} d_{k_1 - 1} \cdots d_0)_{\text{Fibonacci}} \, .$$

b) Verifique que nenhum número inteiro positivo n tem duas representações de Zeckendorf diferentes.

8. Considere o seguinte algoritmo, conhecido como *rotina de Kaprekar*.

1. Escolher, na base decimal, um número de 4 dígitos. Os dígitos não podem ser todos iguais mas o primeiro dígito pode ser 0.
2. Ordenar os dígitos por ordem crescente e por ordem decrescente de modo a obter dois números a quatro dígitos.
3. Subtrair o menor número obtido do maior.
4. Repetir o passo 2.

a) Verifique que, qualquer que seja o número escolhido, o algoritmo de Kaprekar conduz sempre ao número 6174 (designado por *constante de Kaprekar*).

b) O número 6174 é uma constante de Kaprekar de 4 dígitos. Determine as constantes de Kaprekar, i.e. pontos fixos da função de Kaprekar, de n dígitos, para $n = 2, 3, \ldots, 8$. Com alguns valores de n, não vai encontrar constantes de Kaprekar mas ciclos de Kaprekar. Por exemplo, qualquer que seja o número inicial de 2 dígitos, o algoritmo de Kaprekar chega eventualmente ao ciclo

$$09 \to 81 \to 63 \to 27 \to 45 \to 09 \, .$$

c) Determine as constantes e/ou ciclos de Kaprekar de 4 dígitos nas bases $2, 4$ e 16.