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

Matemática Experimental (LMAC) – 1º Semestre de 2019/2020

Trabalho Computacional

1. Um natural n diz-se *número congruente* se ele for igual à área de um triângulo retângulo (pitagórigo) cujos lados são números racionais. Por exemplo, $n = 6$ é um número congruente visto que a área do triângulo de lados $(3, 4, 5)$ é igual a 6. Note-se que se n for congruente então n multiplicado por um quadrado perfeito também é um número congruente. Por exemplo, $24 = 6 \cdot 2^2$ é congruente e corresponde ao triângulo pitagórigo $(6, 8, 10)$ de área 24. Assim, procuram-se apenas números congruentes livres de fatores quadráticos.

a) Verifique que se (a, b, c) for um triângulo pitagórigo de área n, então os quatro pontos

$$(a(a \pm c)/2, a^2(a \pm c)/2)\,, \qquad (b(b \pm c)/2, b^2(b \pm c)/2) \tag{1}$$

são pontos na curva (elíptica) $y^2 = x(x^2 - n^2)$, com $y \neq 0$. Desenhe o gráfico da curva elíptica que corresponde ao número congruente $n = 6$ juntamente com os pontos (1).

b) Prove que se

$$\begin{aligned}&(x, y) = (a(a + c)/2, a^2(a + c)/2), \quad \text{ou} \quad (x, y) = (a(a - c)/2, a^2(a - c)/2), \quad \text{ou}\\&(x, y) = (b(b + c)/2, b^2(b + c)/2), \quad \text{ou} \quad (x, y) = (b(b - c)/2, b^2(b - c)/2),\end{aligned}$$

então o triângulo de lados $a = |x^2 - n^2|/|y|, b = 2n|x/y|, c = (x^2 + n^2)/|y|$ é um triângulo pitagórigo de área n.

c) Os lados (a, b, c) do triângulo retângulo constituem um terno pitagórico. Um terno pitagórico diz-se *primitivo* se $a, b, c > 0$ e $\mathrm{mdc}(a, b) = \mathrm{mdc}(b, c) = \mathrm{mdc}(a, c) = 1$. A fórmula de Euclides

$$(a, b, c) = (k^2 - l^2, 2k\,l, k^2 + l^2)\,, \qquad k, l \in \mathbb{Z} \setminus \{0\}\,,$$

gera ternos pitagóricos. Verifique que estes são primitivos se e só se $k > l > 0$, $\mathrm{mdc}(k, l) = 1$ e $k \not\equiv l \pmod 2$.

d) Escreva um programa `Mathematica` que receba um inteiro $m > 0$ e devolva uma lista de ternos pitagóricos primitivos (a, b, c), com $a \leq b \leq c$, e $a + b + c \leq m$, calculados pela fórmula de Euclides. Teste o seu programa com alguns valores de m entre 20 e 200.

e) Utilize o seu programa da alínea anterior para determinar alguns números congruentes. Considere $k + l \leq 15$ e apresente os resultados numa tabela com cinco colunas em que os valores nas colunas correspondem a:

k
l
o terno pitagórico primitivo (a, b, c)
a área $n = ab/2$
a parte livre de fatores quadráticos de n.

Note que os valores nas duas últimas colunas são números congruentes. Acha este um bom algoritmo para determinar, por exemplo, todos os números congruentes inferiores a 100? Justifique a sua resposta.

f) Prove que $n \in \mathbb{N}$ é congruente se e só se existe um quadrado perfeito racional s^2 tal que $s^2 - n$ e $s^2 + n$ são também quadrados perfeitos, i.e. existe uma progressão aritmética de razão n. Por exemplo, os quadrados perfeitos $1, 25$ e 49 formam uma progressão aritmética de diferença comum 24 e $n = 24$ é um número congruente. Visto que $24 = 6 \cdot 2^2$, dividindo 24 pelo fator quadrático 2^2, obtêm-se os quadrados perfeitos racionais $1/4, 25/4$ e $49/4$ que correspondem à progressão aritmética de diferença comum 6, um número congruente.

g) Prove que o número $n = 1$ é congruente se e só se existirem soluções inteiras positivas $(a, b, c, d) \in \mathbb{N}^4$ para o sistema de equações

$$a^2 + b^2 = c^2\,, \qquad ab = 2d^2\,. \tag{2}$$

Tente verificar (computacionalmente) que o sistema de equações diofantinas (2) não admite soluções inteiras positivas.

h) Seja $n \in \mathbb{N}$ um inteiro positivo sem fatores quadráticos e seja $f(n)$ o número de soluções inteiras para a equação diofantina $x^2 + 2y^2 + 8z^2 = n$, i.e.

$$f(n) = \#\{(x, y, z) \in \mathbb{Z}^3 \,:\, x^2 + 2y^2 + 8z^2 = n\}\,.$$

De igual modo, definem-se os conjuntos

$$\begin{aligned} g(n) &= \#\{(x, y, z) \in \mathbb{Z}^3 \,:\, x^2 + 2y^2 + 32z^2 = n\} \\ h(n) &= \#\{(x, y, z) \in \mathbb{Z}^3 \,:\, x^2 + 4y^2 + 8z^2 = n/2\} \\ k(n) &= \#\{(x, y, z) \in \mathbb{Z}^3 \,:\, x^2 + 4y^2 + 32z^2 = n/2\} \end{aligned}$$

Sabe-se que:

- *se um número ímpar n for congruente então $f(n) = 2g(n)$;*
- *se um número par n for congruente então $h(n) = 2k(n)$.*

Baseando-se neste resultado, defina uma função `Mathematica` que receba um inteiro positivo n e devolva a mensagem *n não é congruente* ou a mensagem *n é possivelmente congruente*. Utilize a sua função para determinar os inteiros $1 \leq n \leq 50$ que poderão ser congruentes e os que não o são.

i) Sejam $g(T)$ e $\theta_j(T), j = 1, 2,$ séries infinitas de potências em T definidas por

$$g(T) = T \prod_{n=1}^{\infty} (1 - T^{8n})\,(1 - T^{16n})\,, \qquad \theta_j(T) = 1 + 2\sum_{n=1}^{\infty} T^{2jn^2}\,, \qquad j = 1, 2\,.$$

Definem-se ainda

$$A(T) := \sum_{n=1}^{\infty} a(n) T^n = g(T)\theta_1(T)\,, \qquad B(T) := \sum_{n=1}^{\infty} b(n) T^n = g(T)\theta_2(T)\,.$$

Seja n um número ímpar positivo sem fatores quadráticos. Se n for congruente então $a(n) = 0$. Se $2n$ for congruente então $b(n) = 0$. Determine, utilizando este critério, todos os inteiros não congruentes inferiores a 100.

j) Se admitirmos que a famosa conjetura de Birch-Swinnerton-Dyer-Tunnell é verdadeira, então as condições das alíneas **h)** e **i)** são também suficientes para garantir que um número n seja congruente. Escreva um programa `Mathematica` que receba um inteiro $n > 0$ e, utilizando um dos critérios das alíneas anteriores, devolva `True` se n for congruente e `False` no caso contrário. Tente determinar os triângulos pitagórigos que correspondem aos primeiros 20 números congruentes.

k) Seja n um inteiro positivo não divisível por um quadrado perfeito. Verifique que se n é da forma

$$n \equiv 5 \pmod 8 \quad \text{ou} \quad n \equiv 6 \pmod 8 \quad \text{ou} \quad n \equiv 7 \pmod 8$$

então ele é congruente.

l) Obtenha Figura 1 desenhando no plano **kl** os pontos que correspondem aos ternos pitagóricos primitivos gerados pela fórmula de Euclides quando $0 < l < k \leq 50$.

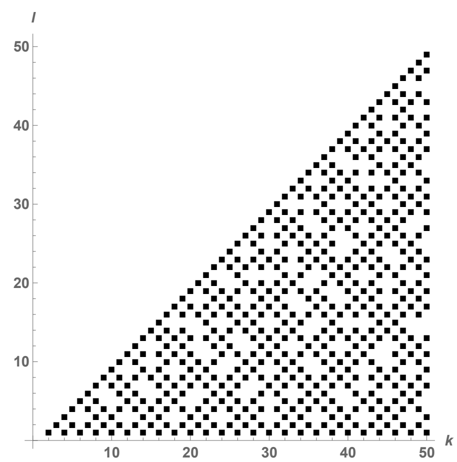

Figura 1: Ternos pitagórigos, com $0 \leq l \leq k \leq 50$

.

2. Um número complexo da forma $a + b\,i$, em que $a, b \in \mathbb{Z}$ e i é a unidade imaginária, diz-se *inteiro gaussiano*. O conjunto de todos os inteiros gaussianos é designado por $\mathbb{Z}[i]$. Ao inteiro $N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2$ chama-se *norma* de $\alpha \in \mathbb{Z}[i]$; $\overline{\alpha} = a - b\,i$ é o *conjugado* de α. Diz-se que $\beta \in \mathbb{Z}[i] \setminus \{0\}$ divide $\alpha \in \mathbb{Z}[i]$, e escreve-se $\beta \,|\, \alpha$, se existir $\gamma \in \mathbb{Z}[i]$ tal que $\alpha = \beta\gamma$. Para $\alpha, \beta, \gamma \in \mathbb{Z}[i]$, escreve-se ainda $\alpha \equiv \beta \pmod{\gamma}$ se $\gamma \,|\, (\alpha - \beta)$.

Os elementos ± 1 e $\pm i$ dizem-se *unidades*; são os únicos elementos invertíveis em $\mathbb{Z}[i]$. Aos elementos $-\alpha$, $i\,\alpha$ e $-i\,\alpha$ chamam-se *associados* de $\alpha \in \mathbb{Z}[i]$. Um inteiro gaussiano α diz-se *primo gaussiano* se os únicos divisores de α em $\mathbb{Z}[i]$ são unidades ou associados de α. Dois inteiros gaussianos α, β dizem-se *primos relativos* e escreve-se $\mathrm{mdc}(\alpha, \beta) = 1$, se os únicos factores comuns de α, β são unidades. Por exemplo 2 não é um primo gaussiano pois $2 = (1 + i)(1 - i)$.

a) Sejam $\alpha, \beta \in \mathbb{Z}[i]$. Mostre que

i. $N(\alpha\beta) = N(\alpha)\,N(\beta)$;

ii. Se $\alpha \,|\, \beta$ em $\mathbb{Z}[i]$ então $N(\alpha) \,|\, N(\beta)$ em $\mathbb{Z}$;

iii. $N(\alpha)$ é um inteiro par se e só se α for um múltiplo de $1 + i$.

b) Seja $p \in \mathbb{N}$ um primo euclidiano. Prove as seguintes afirmações:

i. Se a equação diofantina $x^2 + y^2 = p$ tiver soluções inteiras (x, y) então $\alpha = x + i\,y$ é um primo gaussiano e p não é um primo gaussiano;

ii. Se a equação $x^2 + y^2 = p$ não tiver soluções inteiras então p é um primo gaussiano;

iii. Se $p \geq 3$ e a equação diofantina $x^2 + y^2 = p$ tem soluções então $p \equiv 1 \pmod 4$;

c) Escreva um código `Mathematica` que lhe permita testar a veracidade das afirmações da alínea anterior. Dê exemplos de primos euclidianos que são também primos gaussianos e de primos euclidianos que não são primos gaussianos.

d) Confirme que um inteiro gaussiano $\alpha = a + i\,b$ é primo gaussiano se e só se

(i) α é um primo euclidiano (ou associado de um primo euclidiano) congruente com 3 módulo 4
ou
(ii) $N(\alpha) = a^2 + b^2$ é um primo euclidiano.

e)[**Pequeno Teorema de Fermat para inteiros gaussianos**] Seja $\alpha = a + b\,i$ um inteiro gaussiano e $N(\alpha) = a^2 + b^2$. Se α for um primo gaussiano e β um inteiro gaussiano não divisível por α então

$$\beta^{N(\alpha)-1} \equiv 1 \pmod \alpha .$$

Escreva um programa `Mathematica` que receba $\alpha, \beta \in \mathbb{Z}[i]$ e devolva `True` se a congruência de Fermat for válida.

f) Considere a seguinte construção `Mathematica`

```
ComplexMDC[u_,v_]:=If[v==0,u,ComplexMDC[v,u-v*Round[u/v]]]
```

Interprete o programa e descreva o que cada comando faz. Teste o código tomando diferentes valores de $u, v \in \mathbb{Z}[i]$.

g) Prove que os inteiros gaussianos α, β são primos relativos se e só se existirem $x, y \in \mathbb{Z}[i]$ tais que $1 = x\,\alpha + y\,\beta$.

h) Escreva um programa `Mathematica` que receba um inteiro n e devolva todos os inteiros gaussianos coprimos com n, apresentando-os no plano complexo como na Figura 2.

i) Se o número $(1 + i)^n - 1$ for um primo gaussiano para algum $n \in \mathbb{N}$ então $(1 + i)^n - 1$ diz-se *primo gaussiano de Mersenne*. Determine os primeiros 10 primos gaussianos de Mersenne.

3. Seja f_n o número de Fibonacci de ordem n.

a) Mostre que

$$f_{k+1}^2 - f_k\, f_{k+1} - f_k^2 = (-1)^k , \qquad k = 1, 2, \ldots .$$

b) Mostre que

i. se a equação diofantina $y^2 - yx - x^2 = 1$ tiver soluções $(x, y) \in \mathbb{N} \times \mathbb{N}$ então existe um inteiro positivo k tal que $x = f_{2k}$ e $y = f_{2k+1}$.

i. se a equação diofantina $y^2 - yx - x^2 = -1$ tiver soluções $(x, y) \in \mathbb{N} \times \mathbb{N}$ então existe um inteiro positivo k tal que $x = f_{2k-1}$ e $y = f_{2k}$.

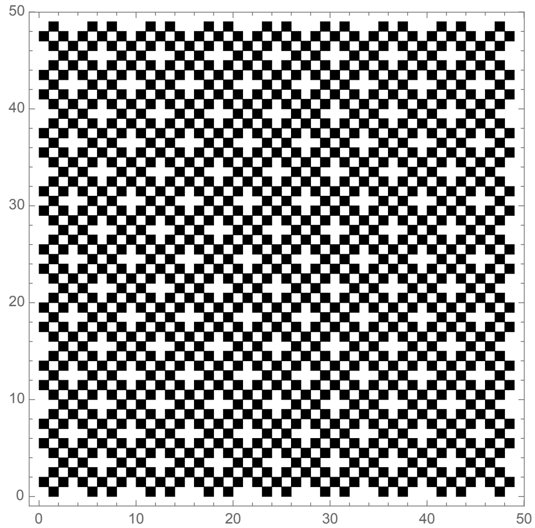

Figura 2: Os inteiros gaussianos coprimos com n=48

.

c) Mostre que a equação diofantina $y^2 - yx - x^2 = 0$ não admite soluções inteiras positivas.

d) Mostre que os números de Fibonacci coincidem com os valores positivos do polinómio

$$p(x,y) = 2y^4x + y^3x^2 - 2y^2x^3 - y^5 - y\,x^4 + 2\,y\,,$$

quando $x = 1, 2, \ldots, y = 1, 2, \ldots$.

4. Implemente o seguinte algoritmo em linguagem `Mathematica`.

Dado k, um inteiro positivo:

1. Determinar os primos p_k, p_{k+1} e p_{k+2} (p_k é o k-ésimo primo);
2. Utilizar o Teorema Chinês dos Restos para achar um inteiro b tal que

   i. b é divisível por $\prod_{i=1}^{k} p_i$;
   ii. $b \equiv -1 \pmod{p_{k+1}}$;
   iii. $b \equiv 1 \pmod{p_{k+2}}$;

3. Devolver a lista $\{b - p_k, \ldots, b-1, b, b+1, \ldots, b+p_k\}$

a) Teste o seu programa com diferentes valores de k. Verifique que $\{b - p_k, \ldots, b-1, b, b+1, \ldots, b+p_k\}$ são números compostos.

b) Explique por que razão o programa devolve $2p_k + 1$ números compostos consecutivos.

5. Verifique que, na base binária, todos os números de Mersenne são da forma $(111\ldots11)_2$. Defina, na base decimal, um número natural por $n = (111\ldots11)_{10}$ e determine os primeiros cinco primos desta forma. Verifique que se $n = (111\ldots11)_{10}$ for primo então o número de dígitos de n é também primo.