Instituto Superior Técnico

Matemática Experimental

1º Semestre - 2019/2020

Licenciatura Em Matemática Aplicada e Computação

Projeto Computacional de Matemática Experimental

Grupo:
José Santos - 85323
Alexandre Silva - 90004
Leandro Duarte - 93112
Vasco Pearson - 97015

Professor:
Juha Videman

18 de Dezembro de 2019

Conteúdo

1 Pergunta 1

1.1 Alínea a)

Queremos verificar se (a, b, c) for um triângulo pitagórico de área n, então os quatro pontos $(a(a \pm c)/2, a^2(a \pm c)/2), (b(b \pm c)/2, b^2(b \pm c)/2)$ pertencem à curva $y^2 = x(x^2 - n^2)$ com $y \neq 0$. Substituindo os pontos na curva obtemos:

$$\frac{a^4(a \pm c)^2}{4} = \frac{a(a \pm c)}{2}\left(\frac{a^2(a \pm c)^2}{4} - \frac{a^2b^2}{4}\right) \iff a(a \pm c) = \frac{(a \pm c)^2 - b^2}{2} \iff$$

$$\iff 2a(a + \sqrt{a^2 + b^2}) = a^2 + 2a\sqrt{a^2 + b^2} + a^2 + b^2 - b^2 \vee$$

$$\vee\ 2a(a - \sqrt{a^2 + b^2}) = a^2 - 2a\sqrt{a^2 + b^2} + a^2 + b^2 - b^2 \iff$$

$$\iff 2a^2 + 2a\sqrt{a^2 + b^2} = 2a^2 + 2a\sqrt{a^2 + b^2} \vee 2a^2 - 2a\sqrt{a^2 + b^2} = 2a^2 - 2a\sqrt{a^2 + b^2}$$

e ainda:

$$\frac{b^4(b \pm c)^2}{4} = \frac{b(b \pm c)}{2}\left(\frac{b^2(b \pm c)^2}{4} - \frac{a^2b^2}{4}\right) \iff b(b \pm c) = \frac{(b \pm c)^2 - a^2}{2} \iff$$

$$\iff 2b(b + \sqrt{a^2 + b^2}) = b^2 + 2b\sqrt{a^2 + b^2} + a^2 + b^2 - a^2 \vee$$

$$\vee\ 2b(b - \sqrt{a^2 + b^2}) = b^2 - 2b\sqrt{a^2 + b^2} + a^2 + b^2 - a^2 \iff$$

$$\iff 2b^2 + 2b\sqrt{a^2 + b^2} = 2b^2 + 2b\sqrt{a^2 + b^2} \vee 2b^2 - 2b\sqrt{a^2 + b^2} = 2b^2 - 2b\sqrt{a^2 + b^2}$$

Podemos então concluir que os quatro pontos pertencem à curva se $c = \sqrt{a^2 + b^2}$ ou seja, se (a, b, c) é um triângulo pitagórico. Verificámos este resultado no Mathematica para alguns valores e para $n = 6$ obtemos a curva elíptica $y^2 = x(x^2 - 36)$ e, como neste caso $(a, b, c) = (3, 4, 5)$, obtemos os pontos $(12, 36), (-3, -9), (18, 72), (-2, -8)$.

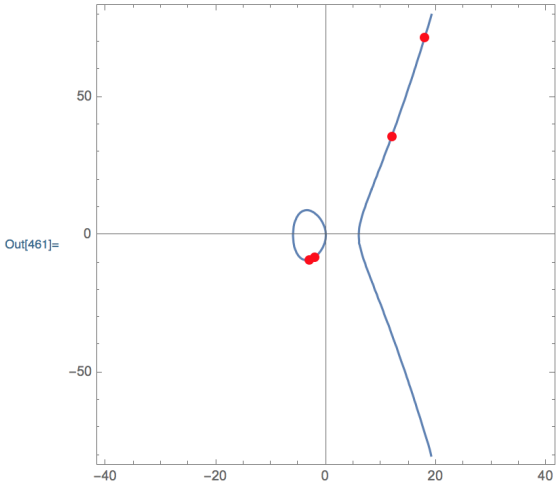

Figura 1: Curva elíptica e os pontos para $n = 6$

1.2 Alínea b)

Seja $(x,y) = (a(a+c)/2, a^2(a+c)/2)$, $(x,y) = (a(a-c)/2, a^2(a-c)/2)$, $(x,y) = (b(b+c)/2, b^2(b+c)/2)$, ou $(x,y) = (b(b-c)/2, b^2(b-c)/2)$, temos que qualquer um destes pontos pertence à curva $y^2 = x(x^2-n^2)$, pela alínea anterior. Sabemos então que $(x^2-n^2) = y^2/x$, portanto

$$a = \frac{|y|}{|x|} = \frac{\frac{y^2}{|x|}}{|y|} = \frac{|x^2-n^2|}{|y|}$$

o que leva a

$$a^2+b^2 = \frac{(x^2-n^2)^2}{y^2} + \frac{4n^2x^2}{y^2} = \frac{x^4-2x^2n^2+n^4+4x^2n^2}{y^2} = \frac{(x^2+n^2)^2}{y^2} = c^2$$

e

$$\frac{1}{2}ab = \frac{2n|y||x|}{2|x||y|} = n$$

Fica assim provado que o triângulo de lados $a = |y/x|, b = 2n|x/y|, c = (x^2+n^2)/|y|$ é um triângulo pitagórico de área n.

1.3 Alínea c)

Demonstração. Considere-se ambas as implicações da equivalência.

$(\implies)$

Seja (a,b,c) um terno pitagórico primitivo gerado pela fórmula de Euclides $(a,b,c) = (k^2-l^2, 2kl, k^2+l^2)$.

Sabemos então que $a,b,c > 0$, logo

$$k^2-l^2 > 0 \iff k^2 > l^2 \iff |k| > |l|$$

e

$$2kl > 0 \iff (k>0 \wedge l>0) \vee (k<0 \wedge l<0)$$

Como os ternos gerados por (k,l) e por $(-k,-l)$ são iguais, basta considerarmos os casos em que $k > l > 0$.

Sabemos também que $mdc(a,b) = mdc(b,c) = mdc(a,c) = 1$. Se $mdc(k,l) = m \neq 1$, teríamos $k = mk'$, $l = ml'$, logo

$$k^2-l^2 = m^2(k'^2-l'^2)$$

$$k^2+l^2 = m^2(k'^2+l'^2)$$

que levaria a

$$mdc(k^2-l^2, k^2+l^2) = m' \geq m^2 > 1$$

o que é absurdo pois pela hipótese temos $mdc(a,c) = mdc(k^2-l^2, k^2+l^2) = 1$
Finalmente, se $k \equiv l(\text{mod } 2)$ temos que $k = l + 2x$, $x \in \mathbb{R}$ logo

$$k^2 + l^2 = (l+2x)^2 + l^2 = l^2 + 4lx + 4x^2 + l^2 = 2(l^2 + 2lx + 2x^2)$$

e

$$k^2 - l^2 = (l+2x)^2 - l^2 = l^2 + 4lx + 4x^2 - l^2 = 2(2lx + 2x^2)$$

e portanto teríamos $mdc(k^2-l^2, k^2+l^2) = mdc(a,c) \geq 2$ o que é absurdo pois $mdc(a,c) = 1$.

($\Longleftarrow$)

Sejam (k,l) tais que $k > l > 0$, $mdc(k,l) = 1$, $k \not\equiv l(\text{mod } 2)$ e sejam (a,b,c) os ternos pitagóricos gerados pela fórmula de Euclides $(a,b,c) = (k^2-l^2, 2kl, k^2+l^2)$.
Como $k > l > 0$ temos que $k^2 > l^2 \iff k^2 - l^2 > 0$, $2kl > 0$, $k^2 + l^2 > 0$, logo $(a,b,c) > 0$.
Devido a $k \not\equiv l(\text{mod}2)$ temos $k \equiv (l-1)(\text{mod}2) \implies k = l - 1 + 2x$. Assim temos que

$$k^2 \pm l^2 = ((l-1) + 2x)^2 \pm l^2 =$$

$$= (l-1)^2 + 4x(l-1) + 4x^2 \pm l^2 =$$

$$= l^2 - 2l + 1 + 4xl - 4x + 4x^2 \pm l^2 =$$

$$2(l^2 - l + 2xl - 2x + 2x^2) + 1 \vee 2(-l + 2xl - 2x + 2x^2) + 1$$

Portanto c= $2(l^2 - l + 2xl - 2x + 2x^2) + 1$ e a=$2(-l + 2xl - 2x + 2x^2) + 1$ são números ímpares e b= $2kl = 2((l-1) + 2x)l = 2(l^2 - l + 2xl)$ é par.
Sabemos que $k \not\equiv l(\text{mod}2)$ e mdc(k,l)=1. Seja $d_1 > 0$ um divisor comum de $k^2 + l^2$ e de $k^2 - l^2$ então d_1 divide a sua soma e a sua diferença, que são respetivamente $2k^2$ e $2l^2$. Como $k^2 + l^2$ e $k^2 - l^2$ são ambos ímpares, d_1 é ímpar, logo $d_1 | k^2$ e $d_1 | l^2$. Como k e l são relativamente primos, k^2 e l^2 também o são, logo $d_1 = 1$ e portanto mdc$(a,c) = 1$.
Seja $d_2 > 0$ um divisor comum de $k^2 + l^2$ e de $2kl$ então d_2 divide a sua soma e a sua diferença, que são respetivamente $k^2 + 2kl + l^2 = (k+l)^2$ e $k^2 - 2kl + l^2 = (k-l)^2$. Logo $d_2 | (k+l)$, $d_2 | (k-l)$ e consequentemente $d_2 | (2k) \iff d_2 | k$ e $d_2 | (2l) \iff d_2 | l$ pois como $k^2 + l^2$ é ímpar, d_2 é ímpar. Como k e l são relativamente primos, $d_2 = 1$ e portanto mdc$(a,b) = 1$.
Seja $d_3 > 0$ um divisor comum de $k^2 - l^2$ e de $2kl$ então como $k^2 - l^2 = (k+l)(k-l)$ é ímpar, d_2 é ímpar e temos um dos 4 casos seguintes:

$$(d_3 | (k+l) \wedge d_3 | k) \vee (d_3 | (k-l) \wedge d_3 | k) \vee (d_3 | (k+l) \wedge d_3 | l) \vee (d_3 | (k-l) \wedge d_3 | l)$$

Olhando para o primeiro caso, como d_3 divide a soma e a diferença de $k + l$ e k chegamos à conclusão que $d_3 | k \wedge d_3 | l$. Analogamente chegamos à mesma conclusão

para os outros casos. Logo como k e l são relativamente primos, $d_3 = 1$ e portanto $\text{mdc}(b, c) = 1$.

Ficam assim demonstradas ambas as implicações da equivalência. □

1.4 Alínea d)

Para esta alínea escrevemos um programa em Mathematica que recebe um inteiro $m > 0$ e devolve 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.

Para isto o programa corre todos os valores inteiros positivos de k,l tais que $l < k$ e se satisfazem as condições da fórmula de Euclides para ternos pitagóricos primitivos, ou seja $k^2 - l^2 < 2kl < k^2 + l^2$, $k^2 - l^2 + 2kl + k^2 + l^2 \leq m$, $\text{mdc}(k^2 - l^2, 2kl) = \text{mdc}(k^2 - l^2, k^2 + l^2) = \text{mdc}(2kl, k^2 + l^2) = 1$ e $k \not\equiv l (\text{mod} 2)$ então adiciona o terno $(k^2 - l^2, 2kl, k^2 + l^2)$ à lista de que vai ser devolvida.

1.5 Alínea e)

k	l	(a,b,c)	n	n livre de fq
2	1	(3,4,5)	6	6
3	2	(5,12,13)	30	30
4	3	(7,24,25)	84	21
5	4	(9,40,41)	180	5
6	5	(11,60,61)	330	330
7	4	(33,56,65)	924	231
7	6	(13,84,85)	546	546
8	5	(39,80,89)	1560	390
8	7	(15,112,113)	840	210
9	4	(65,72,97)	2340	65

Este não é um algoritmo eficiente para determinar todos os números congruentes menores que 100 pois mais de metade dos números congruentes determinados são maiores que 100, logo irão ser necessárias muitas iterações do programa para obter todos os números congruentes desejados. Por outro lado a tabela não é sistemática quanto à aparência de números congruentes menores que 100 na última coluna, ou seja não podemos prever, com base na tabela, quando um número congruente específico irá aparecer, portanto este método de geração de números congruentes não é um bom algoritmo.

1.6 Alínea f)

Demonstração. Considere-se ambas as implicações da equivalência.

$(\implies)$

Seja $n \in \mathbb{R}$ um número congruente então existem $a, b, c \in \mathbb{Q}$ tais que $a^2 + b^2 = c^2$ e $\frac{1}{2}ab = n$, então sejam

$$(r, s, t) = (\frac{b-a}{2}, \frac{c}{2}, \frac{b+a}{2})$$

Podemos verificar que

$$t^2 - s^2 = \frac{(b+a)^2}{4} - \frac{c^2}{4} = \frac{a^2 + b^2 + 2ab - c^2}{4} = \frac{ab}{2} = n$$

e

$$s^2 - r^2 = \frac{c^2}{4} - \frac{(b-a)^2}{4} = \frac{c^2 - a^2 - b^2 + 2ab}{4} = \frac{ab}{2} = n$$

Portanto se n é congruente existe um quadrado perfeito racional s^2 tal que $s^2 - n$ e $s^2 + n$ são também quadrados perfeitos ou seja, existe uma progressão aritmética de razão n.

($\Longleftarrow$)

Seja s^2 um quadrado perfeito racional tal que $s^2 - n$ e $s^2 + n$ são também quadrados perfeitos, então existem $r, s, t \in \mathbb{Q}$ tais que $s^2 - r^2 = n$ e $t^2 - s^2 = n$. Estas igualdades levam a $s^2 = n + r^2 \iff 2s^2 = t^2 + r^2$ e a $t^2 - r^2 = 2n \iff (t-r)(t+r) = 2n$. Isto sugere que $a = (t-r)$ $b = (t+r)$ o que leva a

$$a^2 + b^2 = 2(t^2 + r^2) = 2(2s^2) = (2s)^2$$

portanto sendo $(a, b, c) = (t - r, t + r, 2s)$ temos $a^2 + b^2 = c^2$ e concluímos que n é um número congruente.

Ficam assim demonstradas ambas as implicações da equivalência □

O programa desenvolvido para testar a demonstração devolve o terno (r, s, t), o terno (r^2, s^2, t^2) e devolve a diferença entre t^2 e s^2 e a diferença entre s^2 e r^2. No caso de n ser congruente temos $(r^2, s^2, t^2) = (s^2 - n, s^2, s^2 + n)$ e $t^2 - s^2 = s^2 - r^2 = n$

1.7 Alínea g)

Demonstração. Vamos assumir que existe um triângulo retângulo de área 1, cujos lados são números racionais. Sejam as medidas dos seus lados iguais a a/d, b/d e c/d onde a, b, c e d são inteiros positivos, temos que $a^2 + b^2 = c^2$ e $\frac{1}{2}ab = d^2$. Por outras palavras, se existe um triângulo retângulo racional de área 1 então existe um triângulo pitagórico que tem área igual a um quadrado perfeito (o recíproco é também verdade e obtém-se dividindo as equações atrás por d^2). Fica assim porvado 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

$$a^2 + b^2 = c^2,\ ab = 2d^2$$

. □

No Mathematica fizemos um programa que testa a equação para $0 < a, b, c, d < 50$ e devolve o valor de a, b, c, d se a equação tiver solução. Como o programa não devolve nada, concluímos que a equação não tem soluções no domínio testado.

1.8 Alínea h)

Para este problema começámos por definir 4 funções que devolvem o número de soluções inteiras, para um determinado n, inteiro, de cada uma das equações diofantinas descritas. Criámos, também, uma outra função com recorrência a uma função, utilizada anteriormente, que recebe um n, inteiro e sem fatores quadráticos, e devolve *"n é possivelmente congruente"* se as seguintes condições forem respeitadas, e *"n não é congruente"* caso contrário.

$$\text{Se n for impar e } f[n] = 2g[n]$$
$$\text{Se n for par e } h[n] = 2k[n]$$

1.9 Alínea i)

Neste problema conseguimos verificar que para um número n ímpar sem fatores quadráticos ser congruente, $a(n)$ teria de ser 0 e para um par $b(n)$ também teria de ser 0, logo as suas respetivas potências T com expoente n não vão estar presentes na série correspondente. Nesta alínea com a ajuda da função do *Mathematica* **Series** gerou-se as séries $A[T]$ das potencias de T até 100 para os números ímpares e a série $B[T]$ para os números pares. Criou-se uma lista com os valores dos expoentes da série $A[T]$ e o dobro do valor dos expoentes para a $B[T]$, sendo que $2n$ é que era congruente. Fez-se uma lista AB com todos os valores dos expoentes obtidos em $A[T]$ e $B[T]$ e outra lista com os números de 1 a 100 sem os seus fatores primos, comparou-se estes números com os da lista AB e, caso esta os contivesse, *passaria no teste de congruência* e seriam adicionados a uma lista final com os valores congruentes de 1 a 100.

1.10 Alínea j)

O programa da alínea h) já responde ao que é pretendido nesta alínea, pois esse recebe um número inteiro e devolve *n não é congruente* ou *n é congruente*, tendo assim a funcionalidade adequada ao programa pedido nesta alínea. Sabe-se que um numero congruente é a área de um triângulo pitagórico e que o produto desse número por um quadrado perfeito gera outro triângulo pitagórico. Escolhemos o número congruente "6" como referência, pois este triângulo de área 6 tem lados inteiros, facilitando assim as contas do programa para achar os lados do mesmo. Criou-se a função **Ftriangulos[n]** que através do Teorema de Pitágoras e da formula da área de um triângulo, dada por n, calcula o valor dos lados deste. Fez-se uma outra função

que calcula **Ftriangulos[n]** para os 20 primeiros quadrados perfeitos, devolvendo, assim, *20 triângulos pitagóricos diferentes*.

1.11 Alínea k)

Nesta alínea verificámos computacionalmente para os primeiros 100 inteiros que se n é da forma $n \equiv 5(\text{mod}8)$ ou $n \equiv 6(\text{mod}8)$ ou $n \equiv 7(\text{mod}8)$ então n é congruente. Criámos a função booleana **CongMod** que verifica se n e da forma pretendida. De seguida a função **Congr** retorna a lista dos inteiros menores que 100 que satisfazem as condições da função **CongMod** e são livres de fatores quadráticos. Finalmente, usando o programa da alínea h, concluímos que os números obtidos são todos congruentes.

1.12 Alínea l)

Modificando ligeiramente o programa da alínea d), de modo a obtermos todos os pares (k, l) que correspondem a ternos pitagóricos primitivos. Ao desenhar estes pontos no plano obtemos a seguinte figura:

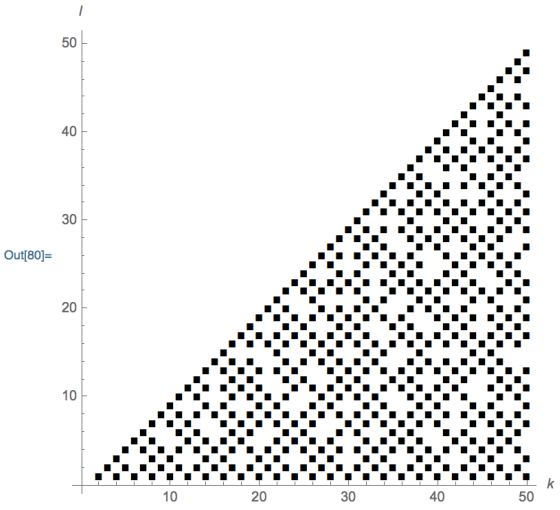

Figura 2: Pontos kl que correspondem a ternos pitagóricos primitivos

2 Pergunta 2

2.1 Alínea a)

Queremos verificar algumas propriedades elementares relativas aos *inteiros gaussianos*, representados pelo conjunto $\mathbb{Z}[i]$.

2.1.1 Sub-Alínea i.

Queremos provar que, dados $\alpha, \beta \in \mathbb{Z}[i]$, e sabendo que $N(\rho) = \rho\overline{\rho} = a^2 + b^2$, em que $\rho \in \mathbb{Z}[i]$, temos que:

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

Demonstração. Sabendo que, em $\mathbb{Z}[i]$, o conjugado do produto é o produto dos conjugados e o produto é comutativo, temos que:

$$N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\alpha}\overline{\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta)$$

□

Para confirmar que esta proposição é verdadeira, foi desenvolvida uma rotina em *Mathematica* que cria (**GenerateGaussNumbers**) e calcula (**NormasProp**) a norma de inteiros gaussianos com $\alpha = a + bi$ e $0 \leq a, b \leq 10$ e testa (função **AllTrue**) se para esses valores a propriedade se verifica (vale notar que ter a ou b negativos iria dar ao mesmo pois são simplesmente associados de um positivo).

2.1.2 Sub-Alínea ii.

Queremos verificar que se $\alpha \mid \beta$ em $\mathbb{Z}[i]$ então $N(\alpha) \mid N(\beta)$ em $\mathbb{Z}$.

Demonstração. Note-se que, por definição, se $\alpha \mid \beta \implies \exists\lambda \in \mathbb{Z}[i] : \beta = \lambda\alpha$, em que $\alpha \in \mathbb{Z}[i] \setminus \{0\}$ e $\beta \in \mathbb{Z}[i]$.
Como $\beta = \lambda\alpha$ implica que $N(\beta) = N(\lambda\alpha)$, podemos aplicar a propriedade demonstrada em **i.**, obtendo:

$$N(\beta) = N(\lambda)N(\alpha)$$

Deste resultado sai que $N(\alpha)|N(\beta)$ em $\mathbb{Z}$, visto que $N(\lambda) \in \mathbb{Z}$, e ainda podemos concluir que existe uma relação estrita entre o inteiro gaussiano múltiplo em $\mathbb{Z}[i]$ e o múltiplo em $\mathbb{Z}$, que corresponde à sua *norma*. □

Para verificarmos esta implicação de um modo prático foi criada uma rotina que confirmava se dois inteiros gaussianos eram divisíveis (**CheckDivisibility**) e caso fossem realizava-se a divisão das normas (**DivisibleGaussNumbers**) e confirmava-se se para todos os casos a divisibilidade das normas se verificava (com a função *AllTrue*).

2.1.3 Sub-Alínea iii.

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

Demonstração. Considere-se ambas as implicações da equivalência.

$(\implies)$

Considere-se $\alpha = a + bi \in \mathbb{Z}[i]$ e $N(\alpha) = a^2 + b^2$ um inteiro par. Como $N(\alpha)$ é um inteiro par, então ou a e b são ambos pares ou a e b são ambos ímpares (pois a soma de dois elementos dá par se e só se ambos os elementos forem pares ou ímpares e apesar de ambos os elementos serem valores ao quadrado, o quadrado de um ímpar é um ímpar e o quadrado de um par é um par). Basta então reparar que:

$$\frac{\alpha}{1+i} = \frac{a+b}{2} + \frac{a-b}{2}i \in \mathbb{Z}[i]$$

Onde se usou a propriedade da divisão dos complexos e o facto de ao terem a mesma paridade, a soma e a subtração ser sempre um valor par e, como tal, divisível por 2, pelo que α é múltiplo de $1 + i$.

$(\impliedby)$

A implicação para a esquerda é obtida de um modo imediato, pois se α é múltiplo de $1 + i$, então $(1 + i) \mid \alpha$, e pela propriedade demonstrada em **ii.**, temos que:

$$1 + i \mid \alpha \implies N(1+i) \mid N(\alpha) \implies 2 \mid N(\alpha)$$

O que equivale a dizer que $N(\alpha)$ é um inteiro par. □

Verificamos esta equivalência recorrendo à função *Equivalent* do Mathematica, para os mesmos inteiros gaussianos da alínea **a)** e recorrendo à função *AllTrue* verificamos para todos os casos que a equivalência se mantém.

2.2 Alínea b)

2.2.1 Sub-Alínea i.

Queremos averiguar que, dada a equação diofantina $x^2 + y^2 = p$, em que $p \in \mathbb{N}$ é um primo euclidiano, tem soluções $(x, y) \in \mathbb{Z}^2$ então $\alpha = x + yi$ é um primo gaussiano e p não é um primo gaussiano.

Demonstração. É fácil verificar que p não é um primo gaussiano, pois dado que $p = x^2 + y^2$ tem soluções e $p \geq 2$ primo euclidiano, então $x + yi$ e $x - yi$ não são nenhuma das identidades de $\mathbb{Z}[i]$.
Para verificarmos que $\alpha = x + yi$ é um primo gaussiano basta ver que:

$$p = x^2 + y^2 = (x + yi)(x - yi)$$

e considerando uma fatorização de $\alpha = x + yi = (a + bi)(c + di)$ podemos verificar que

$$p = x^2 + y^2 = (a^2 + b^2)(c^2 + d^2)$$

Dado que p é primo euclidiano, isto é, p não se pode decompor em mais nenhuma fatorização sem ser a trivial (o que implica que caso apareçam dois termos diferentes, o módulo de um deles têm de ser a unidade), então $a^2+b^2=1$ ou $c^2+d^2=1$. Quer isto dizer que um deles é a identidade e, como tal, apenas temos uma fatorização trivial, pelo que $\alpha = x+yi$ é um primo gaussiano.

□

2.2.2 Sub-Alínea ii.

É-nos pedido agora para verificar se a equação diofantina anterior não tiver soluções, então p é um primo gaussiano.

Demonstração. Prove-se por contrarecíproco. Considere-se que p não era um primo gaussiano, então:

$$\exists \alpha, \beta \in \mathbb{Z}[i] : p = \alpha\beta; p \in \mathbb{N}$$

tal que α e β não são nenhuma das identidades. Usando a primeira propriedade da alínea **a)** deste exercício, podemos verificar que $p = \alpha\beta \Leftrightarrow N(p) = N(\alpha)N(\beta) \Leftrightarrow p^2 = (a^2+b^2)(c^2+d^2)$, em que $\alpha = a+bi$ e $\beta = c+di$. Como, por hipótese, tanto $a^2+b^2 \neq 1$ como $c^2+d^2 \neq 1$, então $p = a^2+b^2 = c^2+d^2$, isto é, a equação diofantina tem soluções. □

2.2.3 Sub-Alínea iii.

Chegadas a estas conclusões é-nos agora pedida uma condição necessária para uma equação diofantina $p = x^2+y^2$, com $p \geq 3$, ter soluções. Vejamos que a equação $p \equiv 1 \bmod 4$ é essa condição.

Demonstração. Considere-se que, para $p \geq 3$, a equação diofantina tem solução e considerem-se os quatro casos possíveis:

$$\begin{cases} p \equiv 0 \bmod 4 \\ p \equiv 1 \bmod 4 \\ p \equiv 2 \bmod 4 \\ p \equiv 3 \bmod 4 \end{cases}$$

É óbvio que sendo p um primo euclidiano, as equações modulares $p \equiv 0 \bmod 4$ e $p \equiv 2 \bmod 4$ não se podem verificar, pois caso elas se verificassem isso significaria que $2 \mid p$ e então p não era um primo, o que entra em contradição com a hipótese inicial. Ficamos então com:

$$\begin{cases} p \equiv 1 \bmod 4 \\ p \equiv 3 \bmod 4 \end{cases}$$

Como queremos resolver a equação diofantina $p = x^2 + y^2$ vejamos todas as hipóteses de valores em módulo 4:

n	0	1	2	3
n^2	0	1	0	1

Portanto as combinações de somas dos n^2, par a par, ou é 0, ou 1, ou 2. Pela razão dada anteriormente e como nunca aparece o caso $p \equiv 3 \bmod 4$ ficamos com necessariamente $p \equiv 1 \bmod 4$.

□

2.3 Alínea c)

Para se verificar a alínea **b)** ***i.*** foi desenvolvida uma rotina que retorna as soluções de $x^2 + y^2 = p$ (*EqDiofantinaSol*), caso contrário retorna vazio. Depois confirmou-se que o inteiro gaussiano dado pela solução era um primo gaussiano (através de *CheckPrimoGaussiano*) e com isso verificamos para os primeiros 300 primos se tal se verificava e que p não era primo gaussiano (*CheckPrimes* e função *AllTrue*).

Para a alínea **b)** ***ii.*** verificou-se, para $p \in [1, 300]$, que quando a equação diofantina não tem soluções inteiras p é primo gaussiano (com a rotina *NonSolutionEDS* e a função *AllTrue*). De notar que a *NonSolutionEDS* é uma função (booleana) que retorna *True* caso tenha soluções ou p não seja primo (pois esses casos não importam para a proposição, e depois quando não tem soluções e p é realmente um primo gaussiano.

Para verificar experimentalmente a implicação **b)** ***iii.*** , verificou-se quando a equação diofantina tem soluções, com p primo euclidiano (com a rotina *SolutionEDS*, onde caso não haja solução ou p não seja primo euclidiano retornam *True*) e verificou-se para $p \in [3, 300]$, recorrendo à função *AllTrue*.

De notar que pelas proposições acima, p é simultaneamente primo euclidiano mas não gaussiano se e só se $p \equiv 1 \bmod 4$ e sabendo que os primos euclidianos e gaussianos são tais que se verifica a congruência $p \equiv 3 \bmod 4$, e como todos os primos são desta forma (exceptuando o 2) podemos reparar que o conjunto $\{3, 7, 11, 19\}$ são primos euclidianos e gaussianos pois são congruentes com $3 \bmod 4$ e o conjunto $\{5, 13, 17\}$ são apenas primos euclidianos pois são congruentes com $3 \bmod 4$. Exemplificou-se no *Mathematica*, para $p \in [3, 50]$, ambos os casos (com a rotina *CheckPrimeGaussAndEuclidian*).

2.4 Alínea d)

É-nos pedida para mostrar agora uma condição necessária e suficiente para que um inteiro gaussiano seja um primo gaussiano.

Demonstração. ($\Longrightarrow$)

Para verificar que esta implicação é verdadeira, isto é, que $a \implies (b \vee c)$ basta reparar que por contra-recíproco temos que $(\neg b \wedge \neg c) \implies \neg a$, isto é, $\neg b \implies \neg a$ e $\neg c \implies \neg a$. A primeira e segunda asserção foram verificadas por contradição.

Mostre-se a primeira implicação. Notamos que este caso acontece com $Im(\alpha) = 0$. Com α primo euclidiano tal que $\alpha \not\equiv 3 \bmod 4$ então obrigatoriamente $\alpha \equiv 1 \bmod 4$. Então queremos ver que caso esta congruência se verifique α não pode ser um primo gaussiano.

Suponha-se, por contradição, que α era primo gaussiano (e como tal euclidiano) $\equiv 1 \bmod 4$. Tendo em conta o critério de Euler (p primo euclidiano e $mdc(a, p) = 1$):

$$a^{(p-1)/2} \equiv 1 \bmod p \textbf{ sse } \text{a é um resíduo quadrático módulo p}$$

Observamos que -1 é resíduo quadrático módulo α, ou seja, $x^2 \equiv -1 \bmod \alpha$, isto é, $\alpha \mid x^2 + 1 \Leftrightarrow \alpha \mid (x - i)(x + i)$. No entanto isto entra em contradição com o facto de α ser um primo gaussiano, pois se α é primo gaussiano então dividia $x + i$ ou $x - i$, isto é, dividia 1 e -1 (as partes reais e imaginárias), o que não é possível. Logo α não pode ser primo gaussiano.

Falta mostrar a segunda implicação (de notar que este caso acontece quando $Im(\alpha) \neq 0$). Assumindo, por absurdo, que se $N(\alpha) = a^2 + b^2 \neq$ primo euclidiano e α fosse primo gaussiano, então $N(\alpha) = wq$ com $|w|, |q| > 1$ e inteiros, isto é, $(a+bi)(a-bi) = wq$. Como $a + bi$ é irredutível então α é associado de w ou q, mas por hipótese $Im(\alpha) \neq 0$ pelo que entramos em contradição.

($\Longleftarrow$) **i)**

Seja α um primo euclidiano (ou seja, $\alpha = a + bi = a$) tal que $\alpha \equiv 3 \bmod 4$. Devido à propriedade demonstrada na alínea **b) iii)** sabemos que a equação diofantina $x^2 + y^2 = \alpha$ tem soluções se $\alpha \equiv 1 \bmod 4$. Logo, se $\alpha \not\equiv 1 \bmod 4$ então a equação diofantina não tem soluções e, dado que α é primo euclidiano então isso necessariamente equivale a ter que se $\alpha \equiv 3 \bmod 4$ então $x^2 + y^2 = \alpha$ não tem soluções. Então, pela alínea **b) ii)** temos que α é um primo gaussiano.

($\Longleftarrow$) **ii)**

Esta implicação é obvia, pois dado que $N(\alpha) = a^2 + b^2$ é primo euclidiano, por **b) i)** temos que $\alpha = a + bi$ é primo gaussiano.

□

Para testar esta condição necessária e suficiente efetuou-se uma rotina que testava a equivalência para inteiros gaussianos com $|\alpha|, |\beta| \leq 100$ (*EquivOfDSLine*) e verificou-se que a função retornava *True* em todos os testes (recorrendo à função *AllTrue*).

2.5 Alínea e)

Para demonstrar o Pequeno Teorema de Fermat para inteiros gaussianos necessitamos de introduzir primeiro o conceito de sistema reduzido de resíduos módulo α. Ao conjunto $A \subset S$, em que S é um *sistema completo de resíduos módulo* α (ou seja, todas as classes de congruência), formado por elementos de S que são coprimos com α chamamos de *sistema reduzido de resíduos módulo* α. Analogamente aos inteiros, o número de elementos desta classe é dada por $\phi(\alpha)$, também conhecida como a *função totiente de Euler* (adaptada a $\mathbb{Z}[i]$).

Demonstração. É óbvio que se α for primo gaussiano então $|A| = |S| - 1$. Mais, pode-se verificar que o número de classes de congruência módulo α é $N(\alpha)$, pelo que $|A| = N(\alpha) - 1$. Para se verificar tal asserção recorre-se a uma proposição da teoria da aritmética de $\mathbb{Z}[i]$, que diz que o sistema completo de resíduos módulo α, α primo gaussiano, tem exatamente $N(\alpha)$ elementos [1].

Seja $A^* = \beta A$. A^* também é um *sistema reduzido de resíduos módulo* α porque o $mdc(\alpha, \beta) = 1$, pelo que cada elemento de A^* é congruente com um e um só elemento de A (em módulo α), isto é, simplesmente ocorreu uma permutação dos elementos de A. Como, dado duas congruências módulo α, a sua multiplicação é também uma congruência módulo α, aplicando a multiplicação das congruências entre os elementos de A^* e A sucessivamente por todos os elementos obtemos:

$$\prod_{i=1}^{N(\alpha)-1} \beta\, a_i \equiv \prod_{i=1}^{N(\alpha)-1} a_i \mod \alpha$$

$$\beta^{N(\alpha)-1} \prod_{i=1}^{N(\alpha)-1} a_i \equiv \prod_{i=1}^{N(\alpha)-1} a_i \mod \alpha$$

O produto pode então ser cancelado e ficamos com:

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

□

Para verificar esta congruência foi criada uma rotina no *Mathematica* que retorna *True* se esta congruência se verificar (*FermatTheoremLGaussians*). Como exemplo verificaram-se os dois casos da equivalência da alínea *d)*. Primeiro considerou-se um primo euclidiano tal que $p \equiv 3 \bmod 4$ (neste caso 7) e considerou-se $\beta = 1 + i$. Depois considerou-se o segundo caso, em que $N(\alpha)$ é primo euclidiano $(5 + 2i)$ e considerou-se $\beta = 2 + 2i$, verificando-se sempre que eram coprimos.

[1] `http://www.fen.bilkent.edu.tr/~franz/nt/ch10.pdf` Proposition 10.

2.6 Alínea f)

A rotina *ComplexMDC* recebe dois inteiros gaussianos u e v e primeiramente verifica se $v = 0$. Caso tal aconteça, o programa termina e retorna u, pois o $mdc(u, 0) = u$. Caso contrário executa outra vez a rotina mas com os parâmetros de entrada $[v, u - v * Round(u/v)]$. A função *Round* retorna o inteiro gaussiano mais próximo da divisão entre u e v. O programa acaba quando se chegar a um caso com $v = 0$. Isto resulta pois $mdc(\alpha, \beta) = mdc(\beta, r)$, em que sabemos pelo Algoritmo da Divisão que $\alpha = q\beta + r$, com $0 \leq N(r) < N(\beta)$ e $\alpha, \beta, q, r \in \mathbb{Z}[i]$, que difere do Algoritmo da Divisão em $\mathbb{Z}$ pois q e r não são únicos [2]. Queremos então mostrar que os seguintes conjuntos (conhecidos na Álgebra por ideais, neste caso do anel de $\mathbb{Z}[i]$) são iguais $\langle \alpha, \beta \rangle = \{x\alpha + y\beta : x, y \in \mathbb{Z}[i]\} = \{a\beta + br : a, b \in \mathbb{Z}[i]\} = \langle \beta, r \rangle$.

Demonstração. Vejamos que ambos os conjuntos se contêm.
($\subset$)
Seja $k \in \langle \alpha, \beta \rangle$. Então $k = x\alpha + y\beta \implies k = x(q\beta + r) + y\beta \implies k = (xq + y)\beta + xr$ pelo que $k \in \langle \beta, r \rangle$.
($\supset$)
Análogo mas com a mudança $r = \alpha - q\beta$. □

Por esta propriedade e pelo facto de os inteiros gaussianos no Algoritmo da Divisão não serem únicos, o que permite arredondar para vários valores (inclusivamente o mais próximo de cada coordenada real e imaginária, daí o uso de *Round*) concluímos que aplicando isto sucessivamente convergimos para a solução, isto é, obtemos num certo ponto $\langle d, 0 \rangle$, em que d é o máximo divisor comum. Na rotina dada r foi escrito como $r = u - qv$, em que q é calculado pela função *Round(u/v)*, que o aproxima.

2.7 Alínea g)

Vamos verificar uma equivalência em $\mathbb{Z}[i]$ que já se verificava em $\mathbb{Z}$ e que simplifica o trabalho com o máximo divisor comum. Para tal fomos provar os dois lados da equivalência:

Demonstração. ($\implies$)

Sejam α e β primos relativos, isto é, $mdc(\alpha, \beta) = 1$ e M o conjunto $M = \{\alpha x + \beta y : x, y \in \mathbb{Z}[i]\}$, e seja $\theta \in M$ um inteiro gaussiano que minimiza $N(\theta)$.
Pelo algoritmo da divisão, existe $m, r \in \mathbb{Z}[i]$ tal que $\alpha = m\theta + r$, com $0 \leq N(r) < N(\theta)$. Temos então:

$$\alpha = m\theta + r \Leftrightarrow r = m\theta - \alpha$$

[2] Polard, H. & Diamond, H.G. The Theory of Algebraic Numbers. 3. Ed. Dover Publications. (2010) (Page 8-9 *Theorem 1.6*)

ou seja, r é uma combinação de α e θ e como $\alpha, \theta \in M$, ou $r \in M$ ou $r = 0$. Como queremos o valor que minimiza C então, dos dois, queremos $N(r) = 0 \Leftrightarrow r = 0$ e como tal, ficamos com $\alpha = m\theta + r = m\theta$. Logo, $\theta \mid \alpha$. Procedendo da mesma maneira para β vemos então que $\theta|\beta$, e sabendo que α e β primos relativos, então θ é uma unidade.

Temos então que:

$$\theta = x\alpha + y\beta \Leftrightarrow 1 = x\alpha\theta^{-1} + y\beta\theta^{-1} \Leftrightarrow 1 = (x\theta^{-1})\alpha + (y\theta^{-1})\beta$$

com $x\theta^{-1}, y\theta^{-1} \in \mathbb{Z}[i]$, associados de x, y.

($\Longleftarrow$)

Esta implicação é imediata. Seja $d = mdc(\alpha, \beta)$ e $1 = \alpha x + \beta y$. Como $d \mid \alpha$ e $d \mid \beta$, então $d \mid 1$, pelo que $d = 1$, a menos de fatores das identidades.

□

Esta equivalência foi verificada computacionalmente recorrendo ao comando *GCD* que calcula o máximo divisor comum entre os inteiros gaussianos e ao comando *Solve*. O conjunto dos pares testados foram $\{(1+i, 3+4i), (2+5i, 2+i), (1+i, 3+3i), (9+15i, 3+3i)\}$. Como é percetível o máximo divisor comum dos primeiros dois pares é 1, enquanto que dos últimos dois são respetivamente $1+i$ e $3+3i$ e, quando se recorre à função Solve, percebe-se que o resultado dos primeiros dois pares têm solução nos inteiros de gauss (basta considerar, respetivamente, $a = 4$ e $a = -2$) no entanto para os últimos dois pares não (no primeiro caso não existe a que torne a parte real de b inteira e no segundo caso isso acontece para ambas as partes).

2.8 Alínea h)

Nesta alínea foi criada uma rotina (*AllCoprimesGaussian*) que dado um inteiro n, calcula os inteiros de gauss com $a, b \leq 10$, com a rotina já usada em várias alíneas (*GenerateGaussNumbers*), e seleciona (com a função *Select*) os inteiros gaussianos coprimos com n. Para transformar este valor da forma complexa para a forma $(a, b) \in \mathbb{R}^2$ usa-se a função *ReIm* do *Mathematica*. Gerou-se então uma grelha de gráficos com a função *GraphicsGrid* para exemplificar para diferentes valores de n.

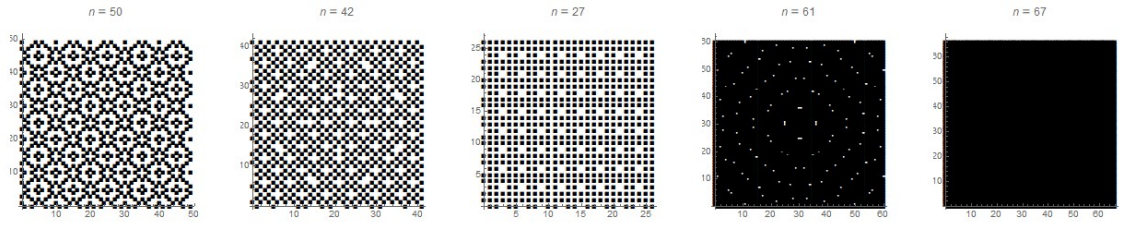

Figura 3: Exemplos para diferentes valores de n os coprimos com este

Podemos observar que os gráficos apresentam simetrias, e são facilmente justificáveis. Nos dois primeiros gráficos, a título exemplificativo, se o $d = mdc(n, \alpha) \neq 1$ então $d \mid n$ e $d \mid \alpha$, e como tal $d \mid n - \alpha$, logo haverá duas zonas brancas simétricas. Isto reflete-se algebricamente para, por exemplo, $n = 50 = 2 \cdot 5 \cdot 5 = 2(2+i)^2(2-i)^2$ em que apresenta vários divisores e como tal vários elementos que não são coprimos e que vão apresentando simetrias.

No terceiro gráfico temos um caso de $n : p^3 = n$, com p primo euclidiano e gaussiano. Sendo p irredutível em $\mathbb{Z}[i]$ então ele só não é coprimo com inteiros gaussianos que se reduzam a $\alpha = 3\beta$, com $\beta \in \mathbb{Z}[i]$, pelo que é de esperar um padrão regular com passo três tanto no eixo dos reais como dos imaginários.

Os últimos dois casos representam um n primo euclidiano mas não gaussiano ($n = 61$) e um primo euclidiano e gaussiano ($n = 67$). No primeiro caso não sendo primo gaussiano sabemos que ele se reduz a $61 = (5+6i)(5-6i)$ Pelo que existem valores em que o $mdc(n, \alpha) \neq 1$. No último é um primo gaussiano logo todos os outros são coprimos com ele, pelo que o gráfico é todo preenchido com quadrados escuros.

2.9 Alínea i)

Nesta alínea são pedidos os primeiros 10 *primos Gaussianos de Mersenne*, que correspondem aos primos gaussianos da forma $(1+i)^n - 1, \quad n \in \mathbb{N}$. Tendo em conta que todos os números da forma $(1+i)^n - 1, \quad n \in \mathbb{N}$ são inteiros Gaussianos, o código utilizado consiste em juntar os 10 primeiros inteiros gaussianos que satisfazem a função **CheckPrimoGaussiano** (utilizada em alíneas anteriores) à lista *mersenneList*; apresentando a mesma de seguida onde são visíveis os 10 valores pedidos.

3 Pergunta 3

Os *números de Fibonacci* formam a denominada **Sequência de Fibonacci** em que cada número resulta da soma dos dois números anteriores.
$f_0 = 0$, $f_1 = 1$,

$$f_n = f_{n-1} + f_{n-2} \quad , n > 1$$

3.1 Alínea a)

Com o objetivo de demonstrar,

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

utilizou-se as propriedades dos *números de Fibonacci* e recorreu-se a uma *Demonstração por Indução*, que segue os seguintes passos:

Demonstração. :

1. Prova-se a igualdade para $n = 1$,

$$f_2^2 - f_1 f_2 - f_1^2 = 1^2 - (1 \times 1) - (1^2) = (-1)^1 \Leftrightarrow -1 = -1$$

2. Assume-se que a igualdade se verifica para $n = k, \quad f_{k+1}^2 - f_k f_{k+1} - f_k^2 = (-1)^k$
3. Usa-se a hipótese para provar a igualdade em $n = k + 1, \quad f_{k+2}^2 - f_{k+1} f_{k+2} - f_{k+1}^2 = (-1)^{k+1}$

$$\begin{aligned} f_{k+2}^2 - f_{k+1} f_{k+2} - f_{k+1}^2 &= f_{k+2}(f_{k+2} - f_{k+1}) - f_{k+1}^2 \\ &= f_{k+2} f_k - f_{k+1}^2 \\ &= (f_k + f_{k+1}) f_k - f_{k+1}^2 \\ &= f_k f_{k+1} + f_k^2 - f_{k+1}^2 \\ &= (-1)(f_{k+1}^2 - f_k f_{k+1} - f_k^2) \\ &= (-1)(-1)^k \\ &= (-1)^{k+1} \end{aligned} \tag{3.1}$$

4. Pelo *Princípio da Indução Matemátca* a igualdade é válida para todos os inteiros de $n \geq 1$, pelo que a prova está completa.

□

Através do programa *Mathematica* usou-se as funções **RightSide** e **AllTrue** para verificar a propriedade de interesse para alguns valores experimentais.

3.2 Alínea b)

Nas seguintes sub-alíneas será utlizada a *Prova Direta* em que se assume **P** Verdadeira e então tenta-se demonstra que **Q** é verdadeira.

3.2.1 Sub-Alínea i.

A *equação diofantina quadrática* $y^2 - yx - x^2 - 1 = 0$ tem o *determinante* da parte quadrática ($\triangle = b^2 - 4ac$) 5. Visto que 5 é positivo e não é quadrado perfeito, então esta é uma equação do tipo *Pell*.

Demonstração. :

1. Assumindo que a equação diofantina $y^2 - yx - x^2 = 1$ tem soluções $(x, y) \in \mathbb{N} \times \mathbb{N}$ então a equação tem infinitas soluções.
2. Considerando $x = f_{2k} \quad _{k \in \mathbb{Z}^+}$, arbitrário, tal que (x, y) é solução da equação.
3. Substituindo $x = f_{2k}$ obtém-se $y^2 - y f_{2k} - f_{2k}^2 = 1$
4. Através da mudança de variável $\lambda = 2k$ obtém-se $y^2 - f_\lambda y - f_\lambda^2 = (-1)^\lambda$, com λ par.
5. Por comparação com a demonstração em *3.1 Alínea a)* verifica-se que $y = f_{\lambda+1}$

6. Invertendo a mudança de variável **conclui-se** $x = f_{2k}$ **e** $y = f_{2k+1}$, como pretendido

□

Através do programa *Mathematica* desenhou-se um gráfico tridimensional da função $j(x, y) = y^2 - yx - x^2$ e do plano $z = 1$ verificando-se que existem soluções $(x, y) \in \mathbb{N}*\mathbb{N}$ e de seguida obteve-se um gráfico bidimensional onde se sobrepõem as soluções inteiras positivas da equação diofantina e os valores de (x, y) da forma $x = f_{2k}, y = f_{2k+1} \quad _{k\in\mathbb{Z}^+}$, donde se conclui que existe um inteiro positivo k que satisfaz a asserção.

3.2.2 Sub-Alínea ii.

À semelhança da anterior, a *equação diofantina quadrática* $y^2 - yx - x^2 + 1 = 0$ é uma equação do tipo *Pell*. Assim, procede-se a uma demonstração semelhante à anterior.

Demonstração. :

1. Assumindo que a equação diofantina $y^2 - yx - x^2 = -1$ tem soluções $(x, y) \in \mathbb{N} \times \mathbb{N}$ então a equação tem infinitas soluções.
2. Considerando $y = f_{2k} \quad _{k\in\mathbb{Z}^+}$, arbitrário, tal que (x, y) é solução da equação.
3. Substituindo $y = f_{2k}$ obtém-se $f_{2k}^2 - f_{2k}x - x^2 = -1$
4. Através da mudança de variável $\lambda = 2k-1$ obtém-se $f_{\lambda+1}^2 - f_{\lambda+1}x - x^2 = (-1)^\lambda$, com λ ímpar.
5. Por comparação com a demonstração em *3.1 Alínea a)* verifica-se que $x = f_\lambda$
6. Invertendo a mudança de variável **conclui-se** $x = f_{2k-1}$ **e** $y = f_{2k}$, como pretendido

□

Através do programa *Mathematica* desenhou-se um gráfico tridimensional da função $j(x, y) = y^2 - yx - x^2$ e do plano $z = -1$ verificando-se que existem soluções $(x, y) \in \mathbb{N} * \mathbb{N}$ e de seguida obteve-se um gráfico bidimensional onde se sobrepõem as soluções inteiras positivas da equação diofantina e os valores de (x, y) da forma $x = f_{2k-1}, y = f_{2k} \quad _{k\in\mathbb{Z}^+}$, donde se conclui que existe um inteiro positivo k que satisfaz a asserção.

3.3 Alínea c)

Para a demonstração desta asserção utilizou-se os resultados obtidos anteriormente e efetuou-se uma prova por contradição.

Demonstração. :

1. Verifica-se que a equação desta alínea pode resultar da *soma das equações* das alíneas **3.2.1** e **3.2.2**,

$$\begin{aligned} &(y^2 - yx - x^2) \quad + \quad (y^2 - yx - x^2) = 1 + (-1) \\ &\Leftrightarrow 2y^2 - 2yx - 2x^2 = 0 \\ &\Leftrightarrow \frac{2y^2 - 2yx - 2x^2}{2} = \frac{0}{2} \\ &\Leftrightarrow y^2 - yx - x^2 = 0 \end{aligned} \tag{3.2}$$

2. Assumindo como verdadeiro que a equação $y^2 - yx - x^2 = 0$ admite soluções inteiras positivas $(x, y) \in \mathbb{N} \times \mathbb{N}$, então (x, y) será solução caso satisfaça ambas as equações $y^2 - yx - x^2 = 1$**(a)** e $y^2 - yx - x^2 = -1$**(b)**.
3. Sendo $x_1 = f_{2k} \quad _{k\in\mathbb{Z}^+}$, se (x_1, y_1) satisfaz a equação **(a)** então, por (3.2.1), $y_1 = f_{2k+1}$.
4. Sendo $x_2 = x_1 = f_{2k} \quad _{k\in\mathbb{Z}^+}$, se (x_2, y_2) satisfaz a equação **(b)** então, por (3.2.2), $y_2 = f_{\frac{4k^2}{2k-1}}$.
5. Por hipótese, $(x_1, y_1) = (x_2, y_2)$ e portanto $2k + 1 = \frac{4k^2}{2k-1} \Leftrightarrow 4k^2 = (2k + 1)(2k - 1) \Leftrightarrow 4k^2 = 4k^2 - 1$, o que é **absurdo**.
6. Conclui-se que a equação $y^2 - yx - x^2 = 0$ **não** admite soluções inteiras positivas $(x, y) \in \mathbb{N} \times \mathbb{N}$, como se queria provar.

□

Através da função **Solve** do *Mathematica*, verificou-se que não existem soluções inteiras positivas para a equação.

3.4 Alínea d)

Nesta alínea desenvolveu-se código no Mathematica com o objetivo de verificar que os *números de Fibonacci* correspondem aos valores positivos do contradomínio da função $p(x, y) = 4y^4x + y^3x^2 - 2y2x^3 - y^5 - yx^4 + 2y$ para valores de x, y naturais. Para tal igualou-se, primeiramente, a função a zero e verificou-se que a propriedade se verifica para os números de Fibonacci excluindo o zero.
A função **vala**[**a**] devolve imagens da função para $(x, y) \in \mathbb{N} \times \mathbb{N}$ e a função **cdp**[**b**] reúne todas essas imagens entre 1 e b.
A função **fibon**[**i**] devolve os primeiros i números de Fibonacci calculados através da *fórmula de Binet* (na função **fbinet**[**n**]).
A demonstração da asserção em questão consiste em verificar que todos os valores de interesse do polinómio **são números de Fibonacci** através da função **demonstracao1**[**s**] e visualizar esta igualdade graficamente com a função **demonstracaoplot**[**v**].

4 Pergunta 4

4.1 Alínea a)

No problema 4 começamos por definir um programa que utiliza a função **Prime** do Mathematica que nos devolve o k-ésimo primo, que usamos para obter p_k, p_{k+1}, p_{k+2}. Definimos o modulo p_i como um produto de primos de p_1 a p_k, como é dito no enunciado, e utilizamos a função **ChineseRemainder** do *Mathematica* que, neste caso, recebe os restos e os módulo $\{0, -1, 1\}, \{p, pk + 1, pk + 2\}$ das congruências e devolve a solução (b) que satisfaz as três equações. Por fim, o programa devolve uma lista de $\{b - pk, ..., b - 1, b, b + 1, ..., b + pk\}$ gerada a partir da solução (b).
Testámos o programa para diferentes valores de k e utilizamos o verificador do Mathematica **CompositeQ** para confirmar que todos os elementos da lista eram compostos.

4.2 Alínea b)

É-nos pedido agora para justificar o facto de o programa devolver $2p_k + 1$ números compostos consecutivos.

Demonstração. Considere-se:

$$\begin{cases} b \equiv 0 \pmod{p} \\ b \equiv -1 \pmod{p_{k+1}} \\ b \equiv 1 \pmod{p_{k+2}} \end{cases}$$

em que $p = \prod_{i=1}^{k} p_k$ que se pode escrever como:

$$\begin{cases} b = q \cdot 2 \cdot 3 \dot{...} \cdot p_k \\ b = -1 + q' \cdot p_{k+1} \\ b = 1 + q'' \cdot p_{k+2} \end{cases}$$

Como b é divisível por um produto de primos *(i)*, $p = p_1, ..., p_k$, b, é divisível por 2, logo b é par, pelo que é composto. Se considerarmos $b + k$, com k primo, então um dos primos que compõem p divide ambos, pelo que p divide $b + k$ (até $b \pm p_k$). Se k for composto, então é composto por um produto de primos, e o mesmo resultado é válido. Finalmente, dado que $p_{k+1} \mid b + 1$ *(ii)*, então $b + 1$ é composto e do mesmo modo $p_{k+2} \mid b - 1$ *(iii)*, então $b - 1$ também é composto. □

5 Pergunta 5

Para escrever qualquer número na base binária, recorre-se à divisão inteira por 2 observando os sucessivos restos da divisão. Logo, todo o número de Mersenne (da forma $2^n - 1$) se escreve $(111...1)_2$ na base binária. Considerando o algoritmo da divisão ($a = qb + r$) demonstra-se recursivamente que,

$$2^n - 1 = 2(2^{n-1} - 1) + 1 \ , \ 2^{n-1} - 1 = 2(2^{n-2} - 1) + 1 \ , \ \dots , \ 2^1 - 1 = 2(1 - 1) + 1$$

Dado que a mudança da base decimal para a base binária é dada pelo resto, todos os números da forma $2^n - 1$ são então da forma $(111...1)_2$. Esta propriedade é também verificada com sucessivos valores de x através da função **BaseForm**[$2^x - 1$,**2**] no *Mathematica*.
Na base decimal, um número natural $x = (1111...11)_{10}$ pode também escrever-se como $\sum_{i=0}^{n} 10^i = \frac{10^{n+1}-1}{9}$. Para mostrar que se um número desta índole for primo então o seu número de dígitos também é primo procedeu-se aos seguintes passos;

Demonstração. Assumindo A $= \underbrace{111\dots111}_{n \text{ digits}} = \frac{10^n-1}{9}$ primo e tendo n como **não** sendo primo, e assim $n = a * b$, $\quad a, b \in \mathbb{Z}$ maiores que 1.

$$\begin{aligned} A = \frac{10^{ab} - 1}{9} &= \frac{(10^a)^b - 1}{9} \\ &= \frac{(10^a - 1)}{9}(1 + (10^a) + (10^a)^2 + \dots (10^a)^{b-1}) \\ &= (1 + 10 + 10^2 + \dots + 10^a)(1 + (10^a) + (10^a)^2 + \dots (10^a)^{b-1}) \end{aligned} \tag{5.1}$$

Visto que $a > 1$, demonstra-se por contradição que n não pode ser composto.
Portanto, **n tem de ser primo**. □