UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

Paula Carolina de Jesus Monteiro

PROBLEMAS SIMPLES COM SOLUÇÕES ENGENHOSAS

Belo Horizonte
2015

Paula Carolina de Jesus Monteiro

PROBLEMAS SIMPLES COM SOLUÇÕES ENGENHOSAS

Monografia apresentada à Comissão Avaliadora para a obtenção de Título de Especialista em Matemática.

Orientadora: Ana Cristina Vieira

Belo Horizonte
2015

Monteiro, Paula Carolina de Jesus.

M775p Problemas simples com soluções engenhosas [manuscrito] / Paula Carolina de Jesus Monteiro. — 2015.
35.f. il.

Orientadora: Ana Cristina Vieira.
Monografia (especialização) - Universidade Federal de Minas Gerais, Instituto de Ciências Exatas, Departamento de Matemática.
Referências 35.

1. Matemática. 2. Álgebra. 3. Matemática – Ensino médio.4. Logarítmos. I. Vieira, Ana Cristina.II. Universidade Federal de Minas Gerais, Instituto de Ciências Exatas, Departamento de Matemática .III.Título.

CDU 51 (043)

Ficha catalográfica elaborada pela bibliotecária Belkiz Inez Rezende Costa CRB 6/1510 Universidade Federal de Minas Gerais - ICEx

ATA DE MONOGRAFIA DO CURSO DE ESPECIALIZAÇÃO EM MATEMÁTICA, APRESENTADA PELA ALUNA PAULA CAROLINA DE JESUS MONTEIRO

Aos doze dias do mês de agosto de 2015, às 10h00, na Sala 2034, reuniram-se os professores abaixo relacionados, formando a Comissão Examinadora homologada pela Comissão do Curso de Especialização em Matemática, para julgar a apresentação da monografia da aluna **Paula Carolina de Jesus Monteiro**, intitulada: *"Problemas Simples com Soluções Engenhosas"*, como requisito para obtenção do Grau de Especialista em Matemática. Abrindo a sessão, a Senhora Presidente da Comissão, Profª. Ana Cristina Vieira, após dar conhecimento aos presentes do teor das normas regulamentares, passou a palavra à aluna para apresentação de seu trabalho. Seguiu-se a arguição pelos examinadores com a respectiva defesa da aluna. Após a defesa, os membros da banca examinadora reuniram-se sem a presença da aluna e do público, para julgamento e expedição do resultado final, com nota 90 e conceito A. Foi atribuída a seguinte indicação: a aluna foi considerada **Aprovada**, por unanimidade. O resultado final foi comunicado publicamente à aluna pela Senhora Presidente da Comissão. Nada mais havendo a tratar, a Presidente encerrou a reunião e lavrou a presente Ata, que será assinada por todos os membros participantes da banca examinadora. Belo Horizonte, 12 de agosto de 2015.

Ana Cristina Vieira

Profª. Ana Cristina Vieira
Orientadora

Maria Cristina Costa Ferreira

Profª. Maria Cristina Costa Ferreira
Examinadora

Prof. André Gimenez Bueno
Examinador

Dedicatória

A Deus, ao meu marido, aos meus pais e familiares, aos meus amigos.

Agradecimentos

Agradeço a Deus pela vida, por me amar e me proporcionar tantas conquistas; ao meu marido e meus pais pelo incentivo e apoio; à minha orientadora Ana Cristina Vieira pela acolhida, incentivo e dedicação; ao aluno Rafael Bezerra dos Santos que, prontamente, me ajudou com as figuras da monografia; aos demais professores do Departamento de Matemática, que colaboraram para a minha formação; aos familiares e amigos pelo apoio.

Resumo

Neste trabalho, apresentamos alguns problemas que têm enunciados simples e bastante interessantes. Os problemas possuem soluções engenhosas e utilizam resultados básicos que são acessíveis a estudantes de ensino médio.

Palavras-chave: álgebra, números inteiros, logaritmos.

Abstract

In this monograph, we present some problems having simple and interesting statements. The problems have ingenious solutions and use basic results which are accessful to high school students.

Keywords: algebra, integer numbers, logarithm.

SUMÁRIO

Introdução

Vamos apresentar três problemas relacionados aos números inteiros e suas propriedades. São problemas curiosos, interessantes, de apresentação simples e que possuem soluções bonitas e elementares. O conhecimento exigido para a resolução destes problemas é dado no Ensino Médio, mas nem sempre os alunos conseguem resolvê-los porque não enxergam a maneira como podem ser resolvidos. Por isso são tão interessantes.

O primeiro problema refere-se a uma propriedade de potência. Seja $S = abcd...k...$ uma sequência de dígitos de 0 a 9. Então existe uma potência, de base natural e diferente de 10, que começa com essa sequência, ou seja, dados uma sequência $S = abcd...k...$ e um número natural $a \neq 10$, existe um número inteiro não negativo n tal que $a^n = abcd...k....$ Vamos provar este resultado para $a = 2$. A solução deste problema consiste em mostrar que existem naturais t e n que satisfazem a inequação $t + \log S \leq n \log 2 < t + \log(S+1)$. Não precisamos encontrar valores para t e n, basta mostrar que eles existem. Para a resolução deste problema usaremos conhecimentos básicos sobre logaritmos e suas propriedades.

O segundo problema refere-se a seguinte propriedade: Dado qualquer número inteiro M de quatro algarismos, desde que seus dígitos não sejam todos iguais, é possível transformá-lo no número 6174, através de uma transformação T aplicada sobre M. Essa transformação é determinada pela subtração de dois números: o primeiro é formado pelos algarismos de M na ordem decrescente e o segundo é formado pelos algarismos de M na ordem crescente. A solução deste problema consiste em mostrar que é possível obter o número 6174 em, no máximo, sete aplicações da transformação T sobre o número M.

O terceiro problema refere-se ao fato de que alguns números inteiros não negativos podem ser escritos como a soma de quadrados de dois inteiros. E essa representação não é única. Existe uma função aritmética que é definida como o número de maneiras pelas quais um número inteiro não negativo pode ser expressado como a soma de quadrados de dois inteiros. Na verdade, essa função corresponde ao número de pares ordenados (x, y), com $x, y \in Z$, que satisfazem a equação $n = x^2 + y^2$. A solução deste problema consiste em mostrar que, em média, um número inteiro não negativo tem π representações como a soma de quadrados de dois inteiros.

Capítulo 1

Uma propriedade de a^n

Neste capítulo vamos mostrar que, dado um número natural a e qualquer sequência S de dígitos de 0 a 9, existe uma potência de a que começa com essa sequência. Esta propriedade é válida para qualquer potência de base natural e diferente de 10. A demonstração será feita para potências de base 2. O caso geral é estabelecido de modo análogo. Começaremos com alguns exemplos.

Exemplo 1.1. Para $S = 3$, temos que $2^5 = \mathbf{3}2$.

Exemplo 1.2. Para $S = 12$, temos que $2^7 = \mathbf{12}8$.

Exemplo 1.3. Para $S = 20$, temos que $2^{11} = \mathbf{20}48$.

Exemplo 1.4. Para $S = 102$, temos que $2^{10} = \mathbf{102}4$.

.

Generalizando: Seja $S = abcd....k$ uma sequência de dígitos de 0 a 9. Nós precisamos provar que existe um número inteiro não negativo n, tal que:

$$2^n = abcd...k....$$

Para fixar as idéias usaremos um exemplo concreto, $S = 5$ (nesse caso $n = 9$, pois $2^9 = 512$). Se 2^n começa com 5 isto pode ocorrer em um dos seguintes intervalos:

$$\begin{array}{llll} (i) & 5 & \leq 2^n < & 6, \\ (ii) & 50 & \leq 2^n < & 60, \\ (iii) & 500 & \leq 2^n < & 600, \\ (iv) & 5000 & \leq 2^n < & 6000, \qquad \text{etc.} \end{array}$$

Podemos expressar cada intervalo da seguinte maneira:

$$\begin{array}{lllll}
(i) & 5.10^0 & \leq 2^n < & (5+1).10^0, & \\
(ii) & 5.10^1 & \leq 2^n < & (5+1).10^1, & \\
(iii) & 5.10^2 & \leq 2^n < & (5+1).10^2, & \\
(iv) & 5.10^3 & \leq 2^n < & (5+1).10^3, & \text{etc.}
\end{array}$$

Em geral, nós temos:

$$\begin{array}{lllll}
(i) & S & \leq 2^n < & (S+1) & \\
(ii) & S.10 & \leq 2^n < & (S+1).10 & \\
(iii) & S.10^2 & \leq 2^n < & (S+1).10^2 & \\
(iv) & S.10^3 & \leq 2^n < & (S+1).10^3 & \\
\vdots & & & & \\
(t+1) & S.10^t & \leq 2^n < & (S+1).10^t & (A)
\end{array}$$

Vamos mostrar que , dada qualquer sequência S, existe algum natural t e algum natural n que satisfaz a inequação (A). Não precisamos nos preocupar em encontrar os valores de t e n, basta demonstrar que eles existem.

Extraindo o logaritmo, na base 10, dos dois lados da inequação (A), temos:

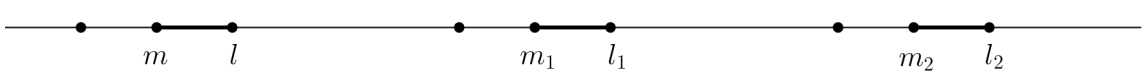
$$\log(S.10^t) \leq \log 2^n < \log[(S+1).10^t]$$

$$\log S + \log 10^t \leq n.\log 2 < \log(S+1) + \log 10^t$$

$$t + \log S \leq n \log 2 < t + \log(S+1) \qquad (B)$$

Qualquer t e n que satisfaz (B) também satisfaz (A).Vamos provar que para qualquer sequência S existem inteiros não negativos t e n que satisfazem (B).

Considere $m = \log S$ e $l = \log(S+1)$ extremos do intervalo $[m, l[$ e, defina $m_k = k + m$ e $l_k = k + l$, onde $k \geq 1$.



$$m = \log S, l = \log(S+1), \ldots, m_k = k + m, l_k = k + l$$

Para $S = 1$, temos $n = 0$, pois $2^0 = 1$.Para $S > 1$, o comprimento do intervalo $[m, l[$ é:

(1) $l - m = \log(S+1) - \log S = \log(\frac{S+1}{S}) = \log(1 + \frac{1}{S}) < \log 2 < 1.$

A cada vez que intervalo é transladado uma unidade para a direita, temos um novo intervalo, o que resulta na seguinte sequência de intervalos:

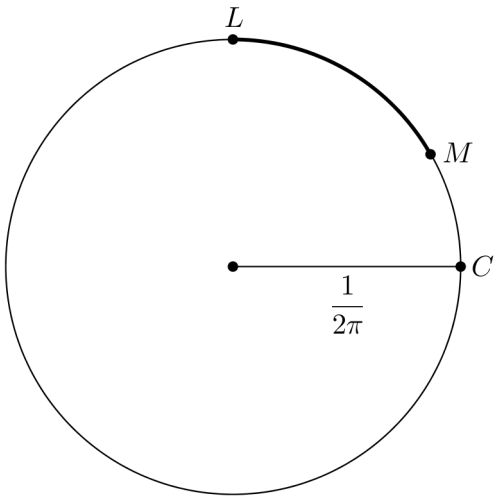
$$[m, l[= [\log S, \log(S+1)[$$

$$[m_1, l_1[= [1 + \log S, 1 + \log(S+1)[$$

$$[m_2, l_2[= [2 + \log S, 2 + \log(S+1)[$$

$$\vdots$$

$$[m_i, l_i[= [i + \log S, i + \log(S+1)[$$



Agora vamos considerar um círculo de comprimento unitário (isto é, de raio $r = \frac{1}{2\pi}$) sendo percorrido, infinitamente, pelos números reais positivos, no sentido anti-horário, a partir de C, onde o zero é mapeado.

Notamos que se dois números diferem por um inteiro, então eles são mapeados no mesmo ponto do círculo e vice-versa. Então vamos considerar que m, m_1, m_2,... são todos mapeados sobre o ponto M e, l, l_1, l_2,... são todos mapeados sobre o ponto L.

Para qualquer número real positivo k, denotamos por $\lfloor k \rfloor$ o maior inteiro que não excede k. Note que o comprimento do arco CK, medido no sentido

anti-horário, tem a propriedade:

$$\text{comprimento de } \overset{\frown}{CK} = k - \lfloor k \rfloor, \tag{2}$$

onde os pontos C e K são, respectivamente, as imagens de 0 e k.

Vamos fazer uma observação sobre o logaritmo de um número natural que será útil no desenvolvimento do restante da demonstração.

A sequência $\{\log n\}_{n\in\mathbb{N}}$ é uma sequência crescente que passa por todos os números naturais:

$$\underbrace{\log 1}_{=0} < \log 2 < \cdots < \log 9 < \underbrace{\log 10}_{=1} < \log 11 < \cdots < \log 99 < \underbrace{\log 100}_{=2} < \cdots$$

Claramente, os números naturais atingidos por esta sequência surgem a partir de logaritmos de potências de 10. De fato, temos que $\log n \in \mathbb{Z}$ se e somente se, n é uma potência de 10.

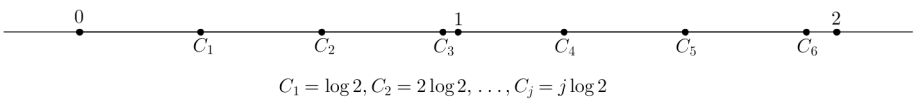
Assim, dado um número natural S, se $S+1$ é uma potência de 10, digamos $S+1 = 10^k, k \in \mathbb{N}$ então $\lfloor \log(S+1) \rfloor = k$. Neste caso, S não é uma potência de 10 e temos que $\log S$ não é inteiro e é tal que $k-1 < \log S < k$. Portanto, $\lfloor \log S \rfloor = k-1$, ou seja,

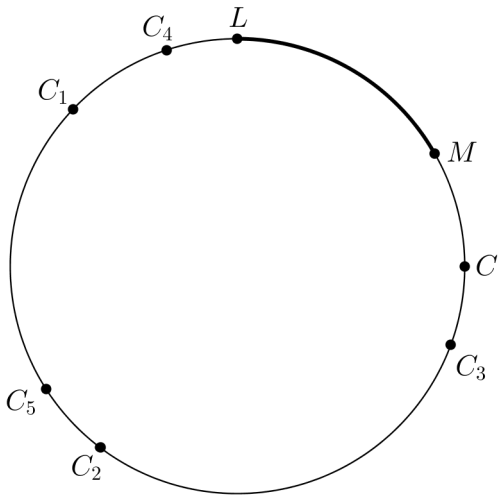
$$\lfloor \log(S+1) \rfloor = \lfloor \log S \rfloor + 1. \tag{3}$$

Por outros lado, se $S+1$ não é uma potência de 10 então $\log(S+1)$ não é inteiro e como $\log S < \log(S+1)$ vamos ter

$$\lfloor \log(S+1) \rfloor = \lfloor \log S \rfloor. \tag{3'}$$

Considere os números $\log 2, 2\log 2, 3\log 2, ..., n\log 2, ...$, e denote suas imagens no círculo por $C_1, C_2, C_3, ..., C_n, ...,$, respectivamente.





Eles estão em volta do círculo e formam arcos de comprimento $\log 2$. Dois deles não coincidem, pois se C_i e C_j $(j > i)$ estivessem mapeados no mesmo ponto,a diferença

$$j \log 2 - i \log 2 = (j - i) \log 2 = w$$

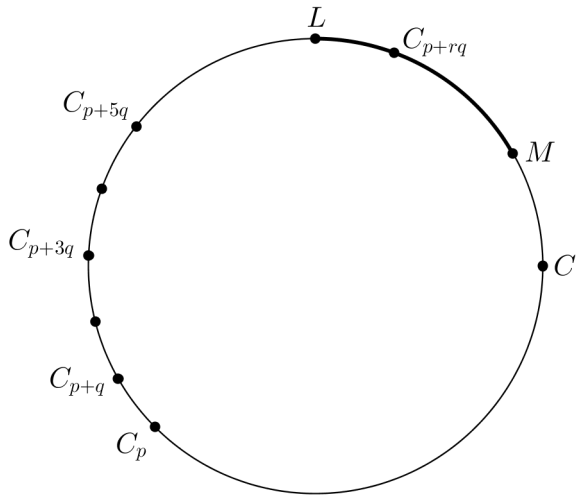
seria um inteiro positivo e, consequentemente, $\log 2 = \frac{w}{j-i}$ seria um número racional, o que é um absurdo. Então todos os pontos C_n são distintos.

Observação: *Se* $\log 2$ *fosse racional, poderíamos escrever* $\log 2 = \frac{u}{v}$ *com* u *e* v *inteiros. Então teríamos* $2 = 10^{\frac{u}{v}}$*, isto é,* $2^v = 10^u$*. Mas isso é impossível porque o lado direito é divisível por 5, enquanto o lado esquerdo não é. Este é o único lugar em que a natureza da base a entra em discussão. Para provar essa propriedade, a só precisa ter um logaritmo irracional.*
Argumentando de um modo semelhante para o caso $a = 2$ *acima, qualquer base que não seja uma potência de 10 pode satisfazer este requisito. Os fatores 2 e 5 nunca são igualmente distribuídos de cada lado da igualdade* $a^v = 10^u$*, a menos que a seja uma potência de 10.*

Existem infinitos pontos C_n. Consequentemente, existe um par desses pontos cuja distância entre eles é menor do que qualquer número pré-fixado. Se, por exemplo, houvesse 100 pontos C_n, é concebível que não há necessariamente dois pontos mais próximos do que $\frac{1}{100}$ (no caso em que os pontos estão uniformemente espaçados). Para a adição de um 101º ponto, no entanto,

seria necessário que a distância entre um par de pontos fosse menor do que $\frac{1}{100}$. Não importa quão pequeno seja o arco $\overset{\frown}{ML}$, mais cedo ou mais tarde os pontos estarão mapeados sobre o círculo de modo que alguns pares estejam a uma distância menor do que o comprimento do arco $\overset{\frown}{ML}$.
Seja C_p e C_{p+q} $(q > 0)$ um par de pontos tal que

(4) $$\text{comprimento de } C_p\overset{\frown}{C}_{p+q} \quad < \quad \text{comprimento de } \overset{\frown}{ML}.$$



Não sabemos se o pequeno arco de C_p para C_{p+q} é no sentido horário ou anti-horário, e isso não importa. Nós olhamos para os pontos

$$C_p, C_{p+q}, C_{p+2q}, ..., C_{p+rq}, ...$$

correspondente aos números

$$p\log 2, (p+q)\log 2, (p+2q)\log 2, ..., (p+rq)\log 2, ...$$

(uma progressão aritmética de razão $q\log 2$) e observamos que

comprimento de $C_p\overset{\frown}{C}_{p+q}$ = comprimento de $C_{p+q}\overset{\frown}{C}_{p+2q}$ = ... = comprimento de $C_{p+(r-1)q}\overset{\frown}{C}_{p+rq}$ = ...;

em outras palavras, esses pontos são mapeados ao redor do círculo (no sentido horário ou anti-horário), em intervalos de comprimento de arco menor que $\overset{\frown}{ML}$, e, por isso, em algum momento, pelo menos um desses pontos

será mapeado dentro do arco $\overset{\frown}{ML}$. Nós podemos concluir que,*dado qualquer número R, não importa quão grande, existe um inteiro $r \geq R$ tal que C_{p+rq} está contido em $\overset{\frown}{ML}$.*
Escolhemos r tão grande que

$$(p + rq)\log 2 \geq \log S \tag{5}$$

em termos de comprimento de arco, nós podemos escrever

$$\text{comprimento de } \overset{\frown}{CM} \leq \text{ comprimento de } \overset{\frown}{CC_{p+rq}} < \text{ comprimento de } \overset{\frown}{CL}, \tag{6}$$

e usando (2), escrevemos assim

$$m - \lfloor m \rfloor \leq (p + rq)\log 2 - \lfloor (p + rq)\log 2 \rfloor < l - \lfloor l \rfloor, \text{ isto é,}$$

$$\log S - \lfloor \log S \rfloor \leq (p+rq)\log 2 - \lfloor (p+rq)\log 2 \rfloor < \log(S+1) - \lfloor \log(S+1) \rfloor. \tag{7}$$

Adicionamos o inteiro $u = \lfloor (p + rq)\log 2 \rfloor$ a todos os membros de (7) e obtemos

$$u + \log S - \lfloor \log S \rfloor \leq (p + rq)\log 2 < u + \log(S + 1) - \lfloor \log(S + 1) \rfloor. \tag{8}$$

Segue de (5) que o inteiro $t = u - \lfloor \log S \rfloor$ é não negativo. Se $(S + 1)$ não é uma potência de 10, nós usamos (3') para deduzir que $t = u - \lfloor \log(S + 1) \rfloor$. Portanto, neste caso, (8) produz a relação desejada

$$t + \log S \leq (p + rq)\log 2 < t + \log(S + 1). \tag{9}$$

No caso em que $(S+1)$ é uma potência de 10, nós observamos que o membro do meio de (7) denota a parte não inteira de $(p + rq)\log 2$ e, portanto, é menor do que 1, então

$$\log S - \lfloor \log S \rfloor \leq (p + rq)\log 2 - u < 1. \tag{7'}$$

Por outro lado, neste caso, (3) resulta em

$$\lfloor \log(S + 1) \rfloor - \lfloor \log S \rfloor = 1,$$

mas como $\log(S + 1) = \lfloor \log(S + 1) \rfloor$, temos que (7') pode ser escrito como

$$\log S - \lfloor \log S \rfloor \leq (p + rq)\log 2 - u < \log(S + 1) - \lfloor \log S \rfloor.$$

Novamente adicionamos u a todos os membros e obtemos o resultado (9) também nesse caso excepcional.

Nós concluímos que, dada qualquer S, existem inteiros t e $n = p + rq$ tal que a inequação (B) é satisfeita. Assim a potência 2^n começa com os dígitos de S.

O resultado de existência que acabamos de provar nos assegura que a busca por uma potência de 2 começando com qualquer sequência de dígitos não é inútil, mas, infelizmente, a prova não nos dá uma receita para construir a potência desejada. Vale a pena notar, conforme o quadro abaixo, que a menor potência de 2 que começa com 7 é 2^{46}, e a menor potência de 2 que começa com 9 é 2^{53}. Potências de 2 começando com qualquer outro dígito são muito pequenas em comparação a estas:

dígito	1	2	3	4	5	6	7	8	9
potência	2^0,2^4	2^8	2^5	2^2	2^9	2^6	2^{46}	2^3	2^{53}

Capítulo 2

O número 6174

Neste capítulo vamos mostrar que, dado um número de quatro algarismos, desde que seus dígitos não sejam todos iguais, é possível transformá-lo no número **6174** por meio de uma transformação, aplicando-a, no máximo, sete vezes. Começaremos com dois exemplos.

Exemplo 2.1. Dado o número 6174, vamos organizar os dígitos de modo a obter o maior número possível, ou seja, vamos colocar os algarismos em ordem decrescente. De maneira análoga, vamos organizar os algarismos de modo a obter o menor número possível. Em seguida vamos subtrair esses dois números:

$$7641 - 1467 = 6174.$$

Exemplo 2.2. Vamos aplicar o mesmo procedimento do exemplo anterior ao número 4959:

$$9954 - 4599 = 5355 \quad \text{o número 6174 não apareceu.}$$

Vamos aplicar o mesmo procedimento ao resultado 5355:

$$5553 - 3555 = 1998 \quad \text{o número 6174 também não apareceu.}$$

Vamos continuar aplicando o procedimento nos resultados:

$$9981 - 1899 = 8082$$
$$8820 - 0288 = 8532$$
$$8532 - 2358 = 6174$$

o número 6174 foi obtido, aplicando-se o mesmo procedimento cinco vezes.

O fato é que, não importa com qual número de quatro dígitos começamos, desde que seus algarismos não sejam todos iguais, o procedimento o transformará no número 6174 em, no máximo, sete passos.

Definição: *Seja M um número de quatro dígitos, não todos iguais. Sejam M_D e M_C números formados pela organização dos algarismos de M na ordem decrescente e crescente, respectivamente. Seja $D_1 = M_D - M_C$. Por esse método nós determinamos para cada número M um número D_1. Essa transformação leva cada número M em um número D_1 e pode ser denotado por T. Nós dizemos*

$$T : M \to D_1 \text{ ou } T(M) = D_1.$$

Devemos mostrar que em, no máximo sete aplicações, a transformação T produzirá o número 6174, isto é,

$$T(M) = D_1, T^2(M) = D_2, ..., T^k(M) = D_k = 6174, \text{ para algum } k \leq 7.$$

Demonstração: Há $10^4 = 10000$ números de quatro dígitos (os números que começam com o algarismo 0 também serão considerados). Mas, desses, existem 10 números (os que têm os quatro dígitos iguais) que são levados no 0000 pela transformação T. Então há 9990 números de quatro dígitos que não possuem todos os algarismos iguais.

Nós vamos mostrar primeiramente que a transformação T leva esses 9990 números em apenas 54 números de quatro dígitos. Sejam a, b, c, d os dígitos de M, tal que

$$(1) \qquad a \geq b \geq c \geq d,$$

desde que as desigualdades não sejam simultaneamente iguais. Vamos calcular $T(M)$:

$$\begin{gathered} M_D = 1000a + 100b + 10c + d \\ M_C = 1000d + 100c + 10b + a \\ D_1 = M_D - M_C = 1000(a-d) + 100(b-c) + 10(c-b) + (d-a) \\ T(M) = 999(a-d) + 90(b-c). \end{gathered}$$

$T(M)$ depende de $(a-d)$ e $(b-c)$. Desde que os dígitos a, b, c, d não sejam todos iguais, a inequação (1) nos dá

$$(2) \qquad a - d > 0 \text{ e } b - c \geq 0,$$

pois se $a = d$ então $a = b = c = d$. Além disso b e c estão entre a e d. $a \geq b \Rightarrow a - d \geq b - d \geq b - c$. Então

$$(3) \qquad a - d \geq b - c$$

As inequações (2) e (3) implicam que $a-d$ pode assumir os valores $\{1, 2, 3, ..., 9\}$ e $b-c$ pode assumir os valores $\{0, 1, 2, 3, ..., a-d\}$. Por exemplo, se $a-d = 1$, as possibilidades para $b - c$ são 0 e 1. Consequentemente, $T(M)$ pode ter apenas os valores

$$999(1) + 90(0) = 0999$$
$$999(1) + 90(1) = 1089$$

Analogamente, se $a - d = 2$, $T(M)$ só pode ter três valores para $b - c$: 0, 1 ou 2. Adicionando o número de valores possíveis para $b - c$ nos casos $a - d = 1, a - d = 2, ..., a - d = 9$ obtemos:

$$2 + 3 + 4 + ... + 10 = 54 \quad \text{possíveis valores para } T(M).$$

		$b-c$									
		0	1	2	3	4	5	6	7	8	9
$a-d$	1	0999	1089								
	2	1998	2088	2178							
	3	2997	3087	3177	3267						
	4	3996	4086	4176	4266	4356					
	5	4995	5085	5175	5265	5355	5445				
	6	5994	6084	6174	6264	6354	6444	6534			
	7	6993	7083	7173	7263	7353	7443	7533	7623		
	8	7992	8082	8172	8262	8352	8442	8532	8622	8712	
	9	8991	9081	9171	9261	9351	9441	9531	9621	9711	9801

Agora observe que dois números M e N que tem os mesmos dígitos, mas não na mesma ordem, tem a mesma imagem de transformação T, ou seja, $T(M) = T(N)$.

Dizemos que dois números são equivalentes se eles têm os mesmos dígitos. Dentre os 54 possíveis valores para $T(M)$ (tabela acima), apenas 30 são não equivalentes. São estes:

0999	1089	1998	2088	2178	2997	3087	3177	3267	3996
4086	4176	4266	4356	4995	5085	5175	5265	5355	5445
6444	7353	7443	8262	8352	8442	9171	9261	9351	9441

Aplicando a transformação T em cada um dos 30 números não equivalentes concluímos que o número 6174 é produzido em, no máximo seis aplicações de T.

número não equivalente	k, para $T^k(M) = 6174$
0999	4
1089	3
1998	3
2088	2
2178	5
2997	5
3087	2
3177	4
3267	5
3996	3
4086	6
4176	1
4266	2
4356	3
4995	5
5085	6
5175	6
5265	4
5355	4
5445	4
6444	4
7353	2
7443	4
8262	4
8352	1
8442	6
9171	2
9261	2
9351	6
9441	6

Antes de finalizar o capítulo, mencionamos que para números de 6 dígitos, existem 384 diferentes resultados possíveis no final da primeira subtração. Dentre estes casos, temos 30 que levam ao "repetidor" 631764, temos 353 que levam ao ciclo $(840852, 860832, 862632, 642654, 420876, 851742, 750843)$

e apenas em um caso o "repetidor" 549945 aparece.

Os resultados para números de 8 dígitos indicam uma conclusão na mesma direção. A similaridade do número de 6 dígitos 631764 com o número 6174 é intrigante e nos faz perguntar se para os próximos casos com número maior de dígitos aparecem os "repetidores" 63317664, 6333176664, etc... Esta é uma questão a se pensar.

Capítulo 3

Escrevendo um número como a soma de dois quadrados

O problema de escrever um número natural como soma de dois quadrados inteiros é bastante antigo. Pierre de Fermat caracterizou tais números ao provar o seguinte teorema.

Teorema (Fermat): Seja n um número natural de modo que sua decomposição em fatores primos seja dada por

$$n = 2^{\gamma} p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}$$

onde os $p_i's$ são primos do tipo $4k+1$ e os $q_j's$ são primos do tipo $4k+3$. Então n é soma de dois quadrados se, e somente se, os $\beta_j's$ são todos pares.

Com isso, nem todo número natural pode ser escrito como soma de dois quadrados inteiros.

Exemplo 3.1. O número 13 é primo do tipo $4k+1$ e $13 = 2^2 + 3^2$.

Exemplo 3.2. Na decomposição do número $15 = 3^1.5^1$, o fator 3 tem expoente ímpar. Portanto, 15 não pode ser escrito como a soma de dois quadrados inteiros.

Exemplo 3.3. Na decomposição do número $42 = 2.3^1.7^1$ os fatores do tipo $4k+3$ (3 e 7), têm expoente ímpar. Portanto, 42 não pode ser escrito como a soma de dois quadrados inteiros.

Exemplo 3.4. Na decomposição do número $90 = 2^1.3^2.5^1$ o fator 3 tem expoente par e $90 = 3^2 + 9^2$.

Neste capítulo vamos observar o que ocorre quando um número natural é escrito como a soma de dois quadrados inteiros.

Na teoria do números há uma função aritmética $r(n)$, definida como o número de maneiras pelas quais um número inteiro não negativo pode ser expressado como a soma de dois quadrados inteiros. Mais precisamente, $r(n)$ é o número de pares ordenados (x, y) , onde $x, y \in \mathbb{Z}$, tais que

$$n = x^2 + y^2.$$

Por exemplo, $r(5) = 8$, pois:

$$\begin{aligned} 5 &= (+1)^2 + (+2)^2 = (+2)^2 + (+1)^2 \\ &= (-1)^2 + (+2)^2 = (+2)^2 + (-1)^2 \\ &= (+1)^2 + (-2)^2 = (-2)^2 + (+1)^2 \\ &= (-1)^2 + (-2)^2 = (-2)^2 + (-1)^2. \end{aligned}$$

Essas expressões correspondem, respectivamente, aos pares ordenados:

$$(1,2), (2,1), (-1,2), (2,-1), (1,-2), (-2,1), (-1,-2), (-2,-1).$$

Alguns valores dessa função são:

$$\begin{aligned} r(0) = 1, \quad r(1) = 4, \quad r(2) = 4, \quad r(3) = 0, \\ r(4) = 4, \quad r(5) = 8, \quad r(7) = 0, \quad r(12) = 0. \end{aligned}$$

Há vários fatos que podem ser provados sobre $r(n)$. Por exemplo, $r(n) = 0$ se n é da forma $4k + 3$, isto é, se n é qualquer número da progressão aritmética 3,7,11,15,19,23,... No apêndice deste texto, vamos comentar este fato e provaremos o teorema que caracteriza os números primos que são soma de dois quadrados.

Mas a função $r(n)$ também pode assumir grandes valores. Não é difícil encontrar um n que vai fazer $r(n)$ ser tão grande quanto se queira. Esta função é extremamente irregular e assim, é uma boa idéia olhar para a média dos valores de $r(n)$. É onde a função é surpreendentemente bem comportada.

Dado um número natural z, a média dos valores de $r(n)$ para $n = 0, 1, ..., z-1$ é:

$$\frac{r(0) + r(1) + r(2) + ... + r(z-1)}{z}.$$

Denotamos o numerador dessa fração por $R(z)$ e a média do valores por $\frac{R(z)}{z}$. A média dos valores de $r(n)$ ao longo dos inteiros não negativos é definida pelo limite da expressão com z tendendo ao infinito

$$\lim_{z\to\infty}\left[\frac{R(z)}{z}\right],$$

desde que o limite exista.

Vamos mostrar que esse limite existe e é igual a π. Em média, um número inteiro não negativo tem π representações como a soma de quadrados de dois inteiros. O interessante é que a prova deste resultado é altamente instrutiva e não é sofisticada. Esta demonstração foi dada pelo matemático alemão Gauss (1777-1855) em torno de 1800, quando ele tinha apenas 23 anos.

Demonstração: No plano cartesiano, considere o círculo

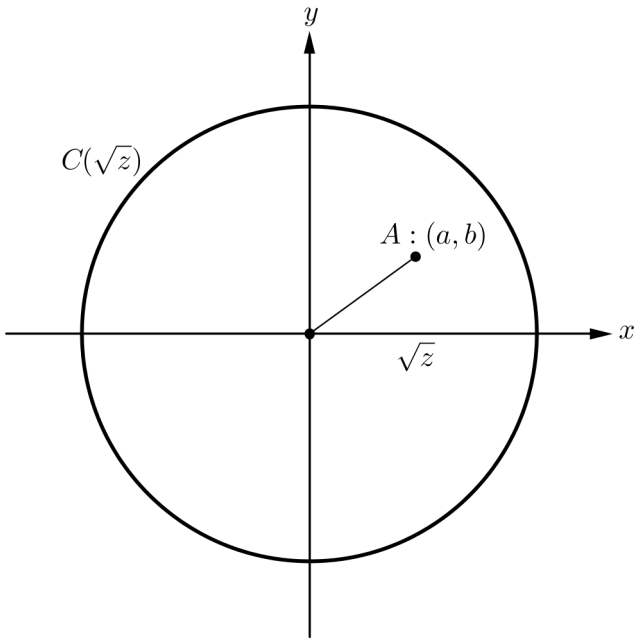
$$C(\sqrt{z}) : x^2 + y^2 = z,$$

com centro na origem e raio $\sqrt{z}$. Seja $A(a, b)$ um ponto reticulado, ou seja, um ponto cujas coordenadas são inteiras. Cada ponto reticulado A dentro de $C(\sqrt{z})$ tem coordenadas satisfazendo a inequação $a^2 + b^2 < z$, desde que a distância de A até a origem seja menor do que o raio de $C(\sqrt{z})$, ou seja,

$$\sqrt{a^2 + b^2} < \sqrt{z}.$$

Além disso, como a e b são inteiros, $a^2 + b^2 = n$ é um número inteiro. Assim o par ordenado (a, b) escreve n como uma soma de dois quadrados.

$$a^2 + b^2 = n < z.$$

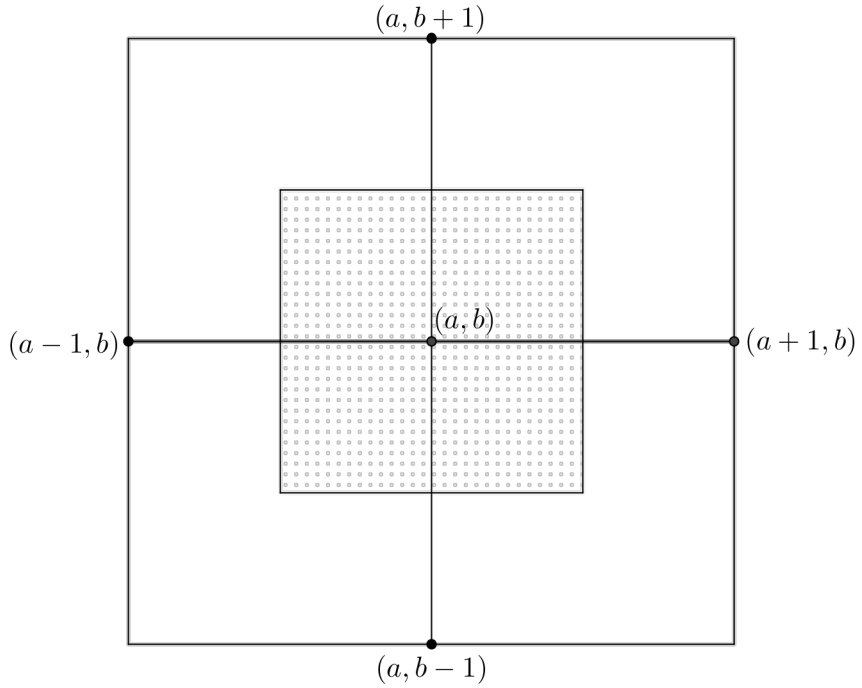


Cada ponto reticulado dentro de $C(\sqrt{z})$ contribui em 1 para a soma $R(z) = r(0) + r(1) + r(2) + ... + r(z-1)$, pois ele fornece um par ordenado contado em algum $r(n)$ em $R(z)$. Reciprocamente, qualquer par ordenado (p, q) tal que

$$p^2 + q^2 = n < z,$$

isto é, qualquer par ordenado contado em algum $r(n)$ em $R(z)$ é um ponto reticulado dentro de $C(\sqrt{z})$. Consequentemente $R(z)$ é igual ao número de pontos reticulados dentro de $C(\sqrt{z})$. Agora nós vamos investigar quantos pontos reticulados há dentro de $C(\sqrt{z})$.

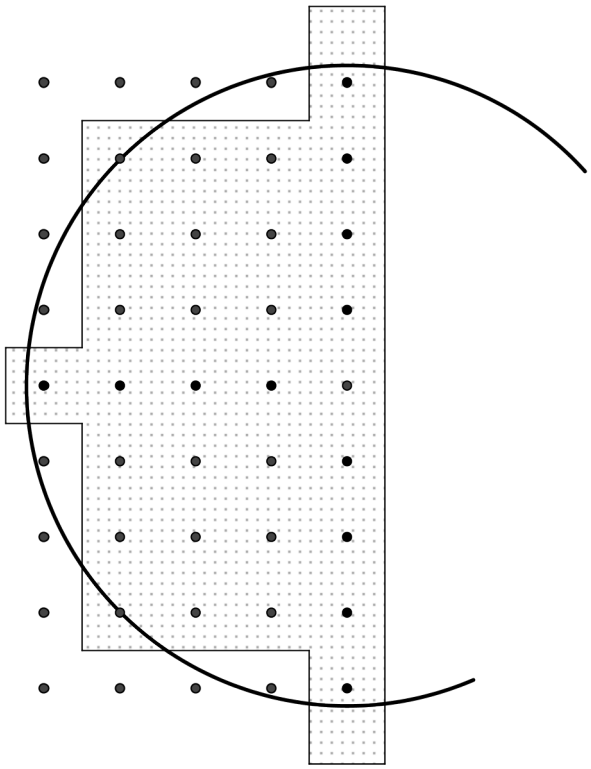
Ao redor de cada ponto reticulado $P(a, b)$ no plano cartesiano, considere um quadrado de lado 1 e centro em P.



Nós colorimos de azul os quadrados com centro em pontos reticulados dentro de $C(\sqrt{z})$ e de vermelho todo os outros quadrados.

Como resultado, a maior parte do interior de $C(\sqrt{z})$ é azul e a maior parte do exterior é vermelho.

Entretanto alguns quadrados azuis são projetados além de $C(\sqrt{z})$ enquanto alguns pedaços de quadrados vermelhos são projetados dentro de $C(\sqrt{z})$.



Agora, o número de quadrados azuis é o número de pontos reticulados dentro de $C(\sqrt{z})$, e é igual a $R(z)$. Além disso, uma vez que cada quadrado tem área igual a 1, o número de quadrados azuis é o total da área colorida de azul, que vamos denotar por A_b. Então

$$R(z) = A_b.$$

Vamos estimar A_b.

Se Q é um ponto reticulado que não está no interior de $C(\sqrt{z})$, e se R é qualquer ponto pertencente ao quadrado com centro em Q, então

$$OQ \geq \sqrt{z}, \qquad RQ \leq \frac{1}{\sqrt{2}},$$

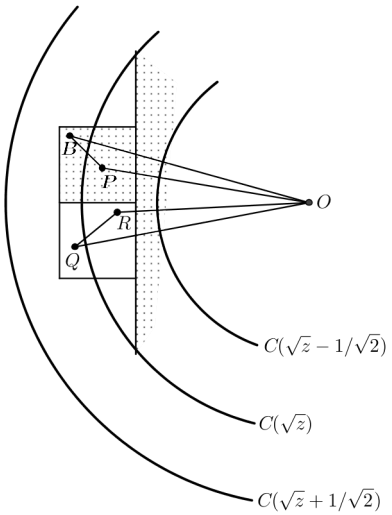
e pela desigualdade triangular, $OR + RQ \geq OQ$, nós temos

$$OR \geq OQ - RQ \geq \sqrt{z} - \frac{1}{\sqrt{2}}.$$

Segue que nenhum ponto colorido de vermelho está dentro do círculo $C\left(\sqrt{z}-\frac{1}{\sqrt{2}}\right)$, com centro na origem e raio $\left(\sqrt{z}-\frac{1}{\sqrt{2}}\right)$. Similarmente, para um ponto B colorido de azul , pertencente a um quadrado com centro no ponto P, nós temos $OP<\sqrt{z}, \quad PB \leq \frac{1}{\sqrt{2}}$, e

$$OB \leq OP + PB < \sqrt{z} + \frac{1}{\sqrt{2}},$$

então nenhum ponto colorido de azul está fora do círculo $C\left(\sqrt{z}+\frac{1}{\sqrt{2}}\right)$.



Segue que a área A_b está entre as áreas dos círculos $C\left(\sqrt{z}-\frac{1}{\sqrt{2}}\right)$ e $C\left(\sqrt{z}+\frac{1}{\sqrt{2}}\right)$:

$$\text{Área } C\left(\sqrt{z}-\frac{1}{\sqrt{2}}\right) \leq A_b = R(z) \leq \text{Área } C\left(\sqrt{z}+\frac{1}{\sqrt{2}}\right),$$

ou seja,

$$\pi\left(\sqrt{z}-\frac{1}{\sqrt{2}}\right)^2 \leq R(z) \leq \pi\left(\sqrt{z}+\frac{1}{\sqrt{2}}\right)^2,$$

$$\pi\left(z-\sqrt{2z}+\frac{1}{2}\right) \leq R(z) \leq \pi\left(z+\sqrt{2z}+\frac{1}{2}\right),$$

$$\pi z-\pi\sqrt{2z}+\frac{\pi}{2} \leq R(z) \leq \pi z+\pi\sqrt{2z}+\frac{\pi}{2},$$

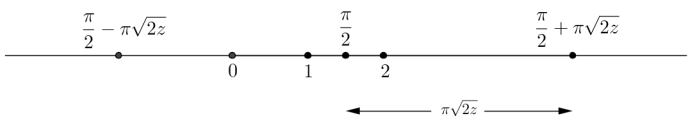
subtraindo πz em todos os membros da desigualdade acima, temos

$$\frac{\pi}{2}-\pi\sqrt{2z} \leq R(z)-\pi z \leq \frac{\pi}{2}+\pi\sqrt{2z},$$

e portanto

$$-\frac{\pi}{2}-\pi\sqrt{2z} \leq R(z)-\pi z \leq \frac{\pi}{2}+\pi\sqrt{2z}.$$

Em outras palavras, o número $R(z)-\pi z$ está dentro do intervalo de $\left(\frac{\pi}{2}-\pi\sqrt{2z}\right)$ a $\left(\frac{\pi}{2}+\pi\sqrt{2z}\right)$, incluindo os seus extremos.



Consequentemente, a magnitude de $R(z)-\pi z$ não pode exceder $\frac{\pi}{2}+\pi\sqrt{2z}$, ou seja,

$$|R(z)-\pi z| \leq \pi\left(\sqrt{2z}+\frac{1}{2}\right),$$

dividindo os termos da inequação por z, temos

$$\left|\frac{R(z)}{z} - \pi\right| \leq \pi\left(\sqrt{\frac{2}{z}} + \frac{1}{2z}\right).$$

À medida que z cresce, a expressão $\pi\left(\sqrt{\frac{2}{z}} + \frac{1}{2z}\right)$ se aproxima de zero. Portanto

$$\lim_{z\to\infty}\left|\frac{R(z)}{z} - \pi\right| = 0,$$

o que é equivalente a

$$\lim_{z\to\infty}\frac{R(z)}{z} = \pi,$$

como queríamos demonstrar.

Apêndice

Primos que são soma de dois quadrados

Queremos caracterizar os números primos em $\mathbb{Z}$ que são soma de dois quadrados. Este é um resultado clássico que foi provado por Pierre de Fermat no Século XVII. Aqui usaremos o que conhecemos do anel dos inteiros gaussianos $\mathbb{Z}[i]$.

O anel $\mathbb{Z}[i]$ é o conjunto

$$\{a + bi \mid a, b \in \mathbb{Z}\}, \quad \text{com} \quad i^2 = -1$$

que é um subanel do corpo dos números complexos $\mathbb{C}$.

Um elemento β em $\mathbb{Z}[i]$ é dito *invertível* se existe um elemento λ em $\mathbb{Z}[i]$ tal que $\beta\lambda = 1$. Os elementos invertíveis de $\mathbb{Z}[i]$ são

$$\{1, -1, i, -i\}.$$

Um elemento não nulo α de $\mathbb{Z}[i]$ é *irredutível* se não é invertível e sempre que escrevemos $\alpha = \beta\gamma$, com β e γ em $\mathbb{Z}[i]$ então β é um elemento invertível ou γ é um elemento invertível em $\mathbb{Z}[i]$. Por exemplo, 5 não é irredutível em $\mathbb{Z}[i]$ pois

$$5 = \underbrace{(2+i)}_{\text{não invertível}} \underbrace{(2-i)}_{\text{não invertível}} .$$

Obs. Podemos provar que se α é irredutível de $\mathbb{Z}[i]$ e $\alpha|\beta\lambda$, com $\beta, \lambda \in \mathbb{Z}[i]$ então $\alpha|\beta$ ou $\alpha|\lambda$, que é uma propriedade comum aos números primos em $\mathbb{Z}$.

Teorema (Fermat): Seja p um primo inteiro. As seguintes afirmações são equivalentes:

1. $p = 2$ ou $p \equiv 1 \pmod 4$
2. existe $a \in \mathbb{Z}$ tal que $a^2 \equiv -1 \pmod p$
3. p não é irredutível em $\mathbb{Z}[i]$
4. p é soma de dois quadrados em $\mathbb{Z}$.

Prova:

(1) ⇒ (2) Se $p = 2$, basta tomar $a = 1$. Agora suponhamos $p \equiv 1 \pmod 4$. Neste caso, $p = 4n + 1$, para algum $n \in \mathbb{Z}$.

Agora, sabemos que se $b \in \mathbb{Z}$ é tal que $mdc(b, p) = 1$ então, pelo Pequeno Teorema de Fermat, $b^{p-1} \equiv 1 \pmod p$, ou seja, $\bar{b}^{p-1} = \bar{1}$ em $\mathbb{Z}_p$, para todo $\bar{b} \in \{\bar{1}, \cdots, p \bar{-} 1\}$. Deste modo, dado $\bar{b} \in \{\bar{1}, \cdots, (p \bar{-} 1)\}$ temos que $\bar{b}$ é raiz do polinômio $x^{p-1} - \bar{1}$ com coeficientes em $\mathbb{Z}_p$:

$$x^{p-1} - \bar{1} = (x - \bar{1})(x - \bar{2}) \cdots (x - (p \bar{-} 1))$$

mas $p - 1 = 4n$ então

$$x^{p-1} - \bar{1} = x^{4n} - \bar{1} = \underbrace{(x^{2n} - \bar{1})}_{grau \;\; 2n = \frac{p-1}{2}} \underbrace{(x^{2n} + \bar{1})}_{grau 2n = \frac{p-1}{2}}.$$

Logo, existe $\bar{b} \in \{\bar{1}, \cdots, p \bar{-} 1\}$ tal que $\bar{b}^{2n} + \bar{1} = \bar{0}$. Fazendo $\bar{a} = \bar{b}^n$ temos $\bar{a}^2 = -\bar{1}$, ou seja, existe $a \in \mathbb{Z}$ tal que $a^2 \equiv -1 \pmod p$, como queríamos mostrar.

(2) ⇒ (3) Suponha que existe $a \in \mathbb{Z}$ tal que $a^2 \equiv -1 \pmod p$. Então $\underbrace{a^2 + 1}_{(a+i)(a-i)} = pk$, para algum $k \in \mathbb{Z}$. Logo,

$$p | (a + i)(a - i), \text{ em } \mathbb{Z}[i].$$

Mas não temos que $p|(a+i)$ e nem que $p|(a-i)$ em $\mathbb{Z}[i]$. De fato, se $p|(a+i)$ então

$$a + i = p(c + di) = pc + pdi \quad \Rightarrow \quad a = pc \qquad \text{e} \qquad \underbrace{1 = pd}_{p \; primo, \; absurdo}$$

e do mesmo modo, chegamos a um absurdo se admitimos que $p|(a - i)$. E assim, p não pode ser um irredutível em $\mathbb{Z}[i]$ de acordo com a observação que fizemos antes do teorema.

(3) ⇒ (4) Suponha que p não seja um irredutível em $\mathbb{Z}[i]$. Então existem $z_1 = a + bi$ e $z_2 = c + di$ em $\mathbb{Z}[i]$ que são elementos não invertíveis tais que $p = z_1 z_2$.

Lembre que z_1 e z_2 são números complexos e assim, suas normas são dadas por $|z_1| = \sqrt{a^2 + b^2}$ e $|z_2| = \sqrt{c^2 + d^2}$. Logo:

$$|p|^2 = |z_1|^2 |z_2|^2 \quad \Rightarrow \quad p^2 = (a^2 + b^2)(c^2 + d^2) \quad \Rightarrow \quad p = a^2 + b^2 = c^2 + d^2$$

ou seja, p é soma de dois quadrados.

(4) $\Rightarrow$ (1) Suponha que p seja soma de dois quadrados e que $p \neq 2$. Neste caso, p é ímpar e vamos mostrar que p deixa resto 1 na divisão por 4. De fato, se deixa resto 3 então temos $p = 4k + 3$ para algum $m \in \mathbb{Z}$.

Agora é simples ver que um número da forma $4k + 3$ não pode ser soma de dois quadrados, pois o quadrado de qualquer inteiro deixa resto 0 ou 1 na divisão por 4 e portanto na soma, o resto deve ser 0, 1 ou 2.

Com isso, provamos que $p \equiv 1 \pmod 4$ e o teorema está provado. Vejamos alguns exemplos.

Exemplo 3.5. Já mencionamos anteriormente que 5 não é irredutível em $\mathbb{Z}[i]$, portanto, de acordo com o teorema acima, ele pode ser escrito como a soma de dois quadrados. Por exemplo, $5 = 1^2 + 2^2$.

Exemplo 3.6. Seja $p = 17$. Ora, $p \equiv 1 \pmod 4$ então, tomando $a = 4$, temos que $a^2 \equiv -1 \pmod p$, ou seja, $4^2 \equiv -1 \pmod{17}$. Portanto 17 não é irredutível em $\mathbb{Z}[i]$ e pode ser escrito como a soma de dois quadrados, por exemplo, $17 = 4^2 + 1^2$.

Exemplo 3.7. Analogamente ao exemplo anterior, para $p = 29$, $p \equiv 1 \pmod 4$. Então, tomando $a = 12$, temos que $a^2 \equiv -1 \pmod p$, ou seja, $12^2 \equiv -1 \pmod{29}$. Portanto 29 não é irredutível em $\mathbb{Z}[i]$ e pode ser escrito como a soma de dois quadrados, por exemplo, $29 = 2^2 + 5^2$.

Exemplo 3.8. Agora, para $p = 7$ temos que $p \equiv 3 \pmod 4$ e p é irredutível, pois $p = 1.7$, sendo que 1 é um elemento invertível de $\mathbb{Z}[i]$. Portanto p não pode ser escrito como a soma de dois quadrados.

Exemplo 3.9. Qualquer número da progressão aritmética 3,7,11,15,19,23,... é da forma $4k + 3$ e, portanto, não pode ser escrito como a soma de dois quadrados.

O Teorema de Fermat que caracteriza os naturais que são soma de dois quadrados inteiros utiliza o teorema que caracteriza os primos que são soma de dois quadrados, mas não faremos a demonstração aqui neste trabalho.

Referências Bibliográficas

[1] A.Garcia e Y.Lequain, **Álgebra: um curso de introdução**, Projeto Euclides - IMPA (1988).

[2] D.Hilbert e S. Cohn-Vossen, **Geometry and the Imagination**, Chelsea, 1952, New York.

[3] R. Honsberger, **Ingenuity in Mathematics**, New Mathematical, sixth edition, 1976.

[4] A.M. Yaglom e I.M. Yaglom, **Challenging Mathematical Problems With Elementary Solutions**, Holden-Day, Inc., 1964, San Francisco.