UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Um estudo sobre a teoria dos números e o último teorema de Fermat

Marina Arantes Barreto

Dissertação de Mestrado do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)

ICMC USP
SÃO CARLOS

Marina Arantes Barreto

Um estudo sobre a teoria dos números e o último teorema de Fermat

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestra em Ciências – Mestrado Profissional em Matemática em Rede Nacional. *EXEMPLAR DE DEFESA*

Área de Concentração: Mestrado Profissional em Matemática em Rede Nacional

Orientadora: Profa. Dra. Michelle Pierri Hernandez

USP – São Carlos
Junho de 2019

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

A273e

Arantes Barreto, Marina
Um estudo sobre a teoria dos números e o último teorema de Fermat / Marina Arantes Barreto; orientador Michelle Pierri Hernandez. -- São Carlos, 2019.
91 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2019.

1. Teoria dos Números. 2. Último Teorema de Fermat. 3. Pitágoras. I. Pierri Hernandez, Michelle, orient. II. Título.

Bibliotecários responsáveis pela estrutura de catalogação da publicação de acordo com a AACR2:
Gláucia Maria Saia Cristianini - CRB - 8/4938
Juliana de Souza Moraes - CRB - 8/6176

Marina Arantes Barreto

A study on number theory and Fermat's theorem

Master dissertation submitted to the Institute of Mathematics and Computer Sciences – ICMC-USP, in partial fulfillment of the requirements for the degree of Mathematics Professional Master's Program. *EXAMINATION BOARD PRESENTATION COPY*

Concentration Area: Professional Master Degree Program in Mathematics in National Network

Advisor: Profa. Dra. Michelle Pierri Hernandez

USP – São Carlos
June 2019

À minha amada filha, Antonella.

AGRADECIMENTOS

Aos meus pais, Mirna e Air, agradeço o amor, o incentivo e o apoio incondicional.

Ao meu marido, Leonardo, que apesar de todas as dificuldades, fortaleceu-me e sempre esteve ao meu lado.

Em especial, agradeço à minha orientadora por todo empenho e dedicação na elaboração desse projeto.

Por fim, a todos que direta ou indiretamente fizeram parte do meu desenvolvimento acadêmico, o meu muito obrigada.

RESUMO

BARRETO, M. A. **Um estudo sobre a teoria dos números e o último teorema de Fermat**. 2019. 91 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2019.

Neste trabalho estudamos alguns dos principais conceitos e propriedades da teoria dos números e apresentamos a história do último teorema de Fermat, bem como o estudo de dois casos particulares desse teorema.

Palavras-chave: teoria dos números; Pitágoras; último teorema de Fermat.

ABSTRACT

BARRETO, M. A. **A study on number theory and Fermat's theorem**. 2019. 91 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2019.

In this work we study some of the main concepts and properties of number theory and present the history of Fermat's last theorem, as well as the study of two particular cases of this theorem.

Keywords: number theory; Pitágoras; Fermat's last theorem.

SUMÁRIO

CAPÍTULO

1

INTRODUÇÃO

A importância da teoria dos números vai além de sua importância na matemática. Os números e suas propriedades fazem parte do nosso dia a dia e, saber lidar com eles é fundamental para a vivência de uma forma geral. Na matemática, a teoria dos números é considerada uma das áreas mais importantes, pois é a base estrutural para todas as outras áreas.

O interesse pelos números e suas propriedades acompanham o desenvolvimento das mais diversas civilizações, desde os momentos iniciais de seus desenvolvimentos. Em particular, no século VI a.C. Pitágoras foi um dos matemáticos mais influentes da época, desenvolvendo a ideia da lógica matemática, das relações entre a matemática e a ciência, dentre outros, sendo assim responsável pelos primeiros avanços importantes da matemática. Também podemos citar, como uma figura essencial para o desenvolvimento da matemática, Euclides que viveu em torno de 300 a.C. Ele escreveu os *Elementos*, o livro-texto mais bem-sucedido de toda a história. Os *Elementos* consistem em treze livros em que a maior parte é voltada para a geometria, mas também aborda conceitos importantes da teoria dos números como, por exemplo, os conceitos de números pares, ímpares, primos e compostos e inicia a regra para a determinação do máximo divisor comum de dois números e a existência de uma quantidade infinita de números primos. No entanto, um matemático que contribuiu ainda mais para a teoria dos números foi Diofanti, que viveu em torno do ano 250. Ele escreveu um livro chamado *Aritmética*, o qual é considerado equivalente aos *Elementos* de Euclides, no entanto, totalmente voltado para a teoria dos números e que trata principalmente da solução de equações indeterminadas com coeficientes inteiros. A *Aritmética* é considerada um dos maiores avanços da teoria dos números e serviu de inspiração para as realizações de outros grandes matemáticos.

No entanto, o mais ilustre dos matemáticos talvez tenha sido Pierre de Fermat (1601-1665), que é considerado o fundador da moderna teoria dos números. Fermat estudou direito em Toulouse, onde trabalhou como conselheiro do parlamento local. No entanto, ele era apaixonado pela matemática, especialmente pela teoria dos números, e esse era seu *hobby* quando não estava

trabalhando. O seu mais famoso resultado, chamado "Último Teorema de Fermat", surgiu em 1637, enquanto estudava um dos livros da *Aritmética* de Diofanti e afirma que não existem números inteiros x, y, z que satisfaçam a equação

$$x^n + y^n = z^n, \quad n \geq 3.$$

Ele não apresentou a prova desse resultado, mas escreveu na margem de sua *Aritmética*: "*Eu tenho uma demonstração realmente maravilhosa para esta proposição, mas esta margem é muito estreita para contê-la.*".

Muitos matemáticos tentaram resolver o problema deixado por Fermat, mas as enormes dificuldades envolvidas para resolvê-lo transformaram o Último Teorema de Fermat num dos maiores desafios intelectuais da história. De fato, as tentativas de solucionar o problema demorou mais de 300 anos e foi resolvido somente em 1994 pelo matemático Andrew Wiles, da Universidade de Princeton. Esse processo fez com que se gerasse uma teoria matemática rica, moderna e diversificada.

Neste trabalho estudamos, inicialmente, alguns dos principais conceitos e propriedades da teoria dos números. Os resultados são apresentados de forma detalhada, esperando que seja um material de fácil leitura e que, ao mesmo tempo, prepare o leitor para a segunda parte deste trabalho, em que estudamos dois casos particulares simples do Último Teorema de Fermat, além de sua história.

A seguir descrevemos, brevemente, os assuntos abordados em cada capítulo.

No Capítulo 2 estudamos algumas propriedades iniciais do conjunto dos números inteiros, tais como o princípio de indução, o teorema do binômio de Newton, os números triangulares e a diferença de dois quadrados. O estudo dessas propriedades foram importantes para o desenvolvimento dos capítulos posteriores. No Capítulo 3 estudamos alguns resultados sobre a teoria da divisibilidade dos números inteiros, incluindo o algoritmo da divisão, o máximo divisor comum, o algoritmo euclidiano e as equações Diofantinas. No Capítulo 4 estudamos alguns dos principais resultados sobre os números primos como, por exemplo, o teorema fundamental da aritmética, o teorema de decomposição primária e a quantidade de divisores de um número, a partir dos números primos. Finalmente, no Capítulo 5 apresentamos, de forma breve, a história do Último Teorema de Fermat e, em seguida, dois casos particulares desse teorema. Especificamente, mostramos que a equação $x^n + y^n = z^n$ não possui solução para o caso $n = 4$ e o caso n=3.

Para o estudo nos Capítulos 2, 3 e 4 utilizamos (MAIER, 2005) e (HEFEZ, 2013) como referências principais. No Capítulo 5, além de (MAIER, 2005), utilizamos as referências (BRUNO, 2014) e (SINGH, 2011).

CAPÍTULO

2

ALGUMAS PROPRIEDADES DOS NÚMEROS INTEIROS

Neste capítulo apresentaremos algumas propriedades do conjunto dos números inteiros $\mathbb{Z} = \{\ldots, -3, -2-1, 0, 1, 2, 3, \ldots\}$, tais como o princípio de indução, o teorema do binômio de Newton, os números triangulares e a diferença de dois quadrados. Essas propriedades serão importantes para o desenvolvimento dos capítulos posteriores.

No que segue usaremos as seguintes notações: $\mathbb{N}_0 = \{0, 1, 2, 3, ...\}$ e $\mathbb{N} = \{0, 1, 2, 3, ...\}$. Além disso, com as operações de adição e multiplicação usuais, consideraremos a ordem natural de $\mathbb{Z}$. Ou seja, dados $m,\ n \in \mathbb{Z}$

$$m \leqslant n \iff n = m + x, \text{ para algum } x \in \mathbb{N}_0.$$

2.1 O princípio da indução

A seguir apresentaremos uma propriedade fundamental do conjunto $\mathbb{N}$.

Princípio da Indução (P.I.): todo conjunto não vazio S de números naturais possui um elemento mínimo. Ou seja, dado $S \subseteq \mathbb{N}$ qualquer, $S \neq \emptyset$, existe $m \in S$ tal que $m \leqslant n$ para todo $n \in S$.

A partir deste princípio podemos demonstrar a seguinte proposição.

Proposição 1. Seja $T \subseteq \mathbb{N}$ tal que

(I) $1 \in T$;

(II) $n \in T \Rightarrow n + 1 \in T$.

Então, T é o conjunto de todos os números naturais, ou seja, $T = \mathbb{N}$.

Demonstração. Suponhamos, por absurdo, que $T \neq \mathbb{N}$. Então, se $S = T^C = \mathbb{N} - T$ temos que $S \neq \emptyset$ e $S \subseteq \mathbb{N}$. Logo segue do P.I. que existe $m \in S$ tal que $m \leqslant n$ para todo $n \in S$.

Agora, pela propriedade (I), $1 \in T$ o que implica que $1 \notin S$ e, portanto, $m > 1$. Logo, considerando o número $\bar{n} = m - 1 < m$ temos que $\bar{n} \in T$. Assim, pela propriedade (II), $\bar{n} + 1 \in T$. Mas, $\bar{n} + 1 = m$, ou seja $m \in T$, o que é absurdo, pois $m \in S = T^C$. Portanto, $T = \mathbb{N}$. □

Observação 1. Considere $T = \{n \in \mathbb{N} | P(n) \text{ vale}\} \subseteq \mathbb{N}$, onde $P(n)$ é uma propriedade envolvendo os números naturais. Então, $n \in T \Rightarrow n + 1 \in T$ é equivalente a $P(n)$ vale $\Rightarrow P(n+1)$ vale. Logo pela Proposição 1 se $1 \in T$, isto é, se $P(1)$ vale e $P(n)$ vale $\Rightarrow P(n+1)$ vale então $T = \{n \in \mathbb{N} | P(n) \text{ vale}\} = \mathbb{N}$, isto é, $P(n)$ vale, para todo $n \in \mathbb{N}$.

Segue da observação acima que para verificar uma propriedade envolvendo números naturais podemos usar a Proposição 1 da seguinte forma.

Proposição 2. Seja $T = \{n \in \mathbb{N} | P(n) \text{ vale}\}$ satisfazendo as seguintes propriedades

a) $P(1)$ vale

b) Se $P(n)$ vale, então $P(n+1)$ vale Então, $T = \mathbb{N}$. Ou seja, $P(n)$ vale para todo $n \in \mathbb{N}$.

Exemplo 1. Vale a seguinte propriedade para todo $n \in \mathbb{N}$

$$1 + 3 + 5 + ... + (2n-3) + (2n-1) = n^2$$

Chamaremos $1 + 3 + 5 + ... + (2n-3) + (2n-1) = n^2$ de $P(n)$

Para $n = 1$, temos que $1 = 1^2$, ou seja, $P(1)$ vale .

Suponha que $P(n)$ seja verdadeiro. Ou seja, suponha que

$$1 + 3 + 5 + \cdots + (2n-3) + (2n-1) = n^2.$$

Somando $(2n+1)$ nos dois membros, temos que

$$1 + 3 + 5 + ... + (2n-3) + (2n-1) + (2n+1) = n^2 + (2n+1).$$

Como podemos reescrever o primeiro termo na forma

$$1+3+5+...+(2n-3)+(2n-1)+(2n+1) = 1+3+5+...+(2(n+1)-3)+(2(n+1)-1),$$

temos que

$$1+3+5+...+(2(n+1)-3)+(2(n+1)-1) = 1+3+5+...+n^2+2n+1 = (n+1)^2,$$

o que prova que $P(n+1)$ vale, ou seja, $P(n) \Rightarrow P(n+1)$. Dessa forma, $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Exemplo 2. Para todos os números naturais n e todo real $a \neq 1$ vale a seguinte propriedade.

$$P(n): 1+a+a^2+a^3+...+a^{n-1}+a^n = \frac{a^{n+1}-1}{a-1}$$

Verifiquemos a validade da igualdade para $n = 1$. Temos que

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

Logo $P(n)$ é verdadeiro para $n = 1$.

Suponha agora que $P(n)$ seja verdadeira para algum $n \in \mathbb{N}$. Ou seja,

$$1+a+a^2+a^3+...+a^{n-1}+a^n = \frac{a^{n+1}-1}{a-1}.$$

Somando a^{n+1} em ambos os membros da igualdade acima temos

$$1+a+a^2+a^3+...+a^{n-1}+a^n+a^{n+1} = \frac{a^{n+1}}{a-1} + \frac{a^{n+1}}{a} = \frac{a^{n+1}-1+a^{n+1}(a-1)}{a-1},$$

ou seja, temos que

$$1+a+a^2+a^3+...+a^{n-1}+a^n+a^{n+1} = \frac{a^{(n+1)+1}-1}{a-1},$$

o que prova que $P(n+1)$ vale. Assim, $P(n) \Rightarrow P(n+1)$. Dessa forma, $P(n)$ é verdadeiro para todo $n \in \mathbb{N}$.

Exemplo 3. Para todos os números naturais n vale a seguinte propriedade.

$$P(n): 1+2+3+...+n = \frac{n(n+1)}{2}.$$

Verifiquemos a validade da igualdade para $n = 1$. Temos que

$$1 = \frac{2}{2} = \frac{1\cdot(1+1)}{2}.$$

Portanto $P(n)$ agora é verdadeira para $n = 1$.

Suponha agora que $P(n)$ seja verdadeira para algum $n \in \mathbb{N}$, ou seja,

$$1+2+3+...+n = \frac{n(n+1)}{2}.$$

Somando $(n+1)$ em ambos os lados da igualdade, temos:

$$1+2+3+...+n+n+1 = \frac{n(n+1)}{2} + (n+1) = \frac{n^2+3n+2}{2} = \frac{(n+1)(n+2)}{2},$$

ou seja, temos que

$$1+2+3+...+n+(n+1)=\frac{n+1[(n+1)+1]}{2},$$

o que prova que $P(n+1)$ vale.

Assim, $P(n) \Rightarrow P(n+1)$. Dessa forma, $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Proposição 3. Seja $n_0 \in \mathbb{Z}$ um inteiro fixo e seja $T' \subseteq \{n \in \mathbb{Z}/n \geqslant n_0\}$. Se o conjunto T' satisfaz as seguintes propriedades:

a) $n_0 \in T'$;

b) $n \in T' \Rightarrow n+1 \in T'$;

então $T' = \{n \in \mathbb{Z}/n \geqslant n_0\}$.

Demonstração. Note que se $n \geqslant n_0$, então $n-n_0+1 \geqslant 1$. Ou seja, $n-n_0+1 \in \mathbb{N}$ para todo $n \geqslant n_0$. Logo, podemos aplicar a Proposição 2 sobre o conjunto

$$T = n-n_0+1/n \in T' \subseteq \mathbb{N}.$$

Inicialmente, como $n_0 \in T'$, temos que $1 = n_0-n_0+1 \in T$. Além disso, se $(n+1) \in T'$, então $n \in T'$ e, por (b), $(n+1) \in T'$. Logo, $(n+1)-n_0+1 \in T$ e, pela Proposição 2, temos que $T = \mathbb{N}$.

Mostremos que

$$A = \{n \in \mathbb{Z}/n \geqslant n_0\} \subseteq T'.$$

Seja $n \in A$. Então, como $n \geqslant n_0$ temos que $n-n_0+1 \in \mathbb{N}$. Assim, como $\mathbb{N} = T$ temos ainda que

$$n-n_0+1 = m-n_0+1$$

para algum $m \in T'$. Ou seja, $n = m \in T'$. Portanto $n \in T'$ e, assim $A \subseteq T'$, o que implica que $T' = A = n \in \mathbb{Z}/n \geqslant n_0$. □

Observação 2. Note que fazendo $n_0 = 1$ na Proposição 3 obtemos a Proposição 1.

Exemplo 4. Mostre que $2^n > n^2$, para $n \geqslant 5$

Para $n = 5$, temos que $2^5 = 32 > 25 = 5^2$. Portanto a propriedade vale para $n = 5$.

Suponha que a propriedade seja verdadeira para algum $n \geqslant 5$. Então,

$$\begin{aligned} 2^{n+1} &= 2^n \cdot 2 > 2n^2 \\ &= n^2+n^2 \\ &= n^2+n \cdot n \\ &\geqslant n^2+5n \\ &= n^2+2n+3n \\ &\geqslant n^2+2n+1 \\ &= (n+1)^2. \end{aligned}$$

Portanto, $2^{n+1} > (n+1)^2$. Logo, pela propriedade 3 a propriedade vale para todo $n \geqslant 5$.

2.2 O teorema binomial

Se $n \in \mathbb{N}_0$ entendemos por n! o produto

$$n! = \prod_{k=1}^{n} k = 1 \times 2 \times 3 \times ... \times n, \text{ se n} \in \mathbb{N}$$

e acrescentamos para $n = 0$, $0! = 1$

Definição 1. Para todo $n \in \mathbb{N}$ e todo $k \in \mathbb{N}_0$, dizemos que com $0 \leqslant k \leqslant n$.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

é o coeficiente binomial n sobre k.

Proposição 4. Para todo $n \in \mathbb{N}$ e todos os $k \in \mathbb{N}_0$ com $0 \leqslant k \leqslant n$, valem as seguintes propriedades.

a) $\binom{n}{k} = \frac{n \cdot (n-1) \cdot ... \cdot (n-k+1)}{k!}$;

b) $\binom{n}{k} = \binom{n}{n-k}$;

c) $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$, se $k \geqslant 1$.

Demonstração. Para o item (a) temos

$$\begin{aligned}
\binom{n}{k} &= \frac{n!}{k!(n-k)!} \\
&= \frac{n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (n-k+2) \cdot (n-k+1) \cdot (n-k) \cdot (n-k-1) \cdot \cdots \cdot 3 \cdot 2 \cdot 1}{k!(n-k)!} \\
&= \frac{n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (n-k+2) \cdot (n-k+1) \cdot (n-k)!}{k!(n-k)!} \\
&= \frac{n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (n-k+2) \cdot (n-k+1)}{k!}.
\end{aligned}$$

Para o item (b) como $0 \leqslant k \leqslant n$, com $n \in \mathbb{N}$ e $k \in \mathbb{N}_0$, temos $0 \leqslant n-k \leqslant n$. Logo

$$\binom{n}{n-k} = \frac{n!}{(n-k)!(n-[n-k])!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}.$$

Para o item (c) temos que

$$\begin{aligned}
\binom{n}{k}+\binom{n}{k-1} &= \frac{n!}{k!(n-k)!}+\frac{n!}{(k-1)!(n-[k-1])!}\\
&= \frac{n!}{k!(n-k)!}+\frac{n!}{(k-1)!(n-k+1)!}\\
&= \frac{n!}{k(k-1)!(n-k)!}+\frac{n!}{(k-1)!(n-k+1)(n-k)!}\\
&= \frac{n!(n-k+1)+k\cdot n!}{k(k-1)!(n-k+1)(n-k)!}\\
&= \frac{n!(n+1)}{k!(n-k+1)!}\\
&= \frac{(n+1)!}{k![(n+1)-k]!}=\binom{n+1}{k}.
\end{aligned}$$

□

Observação 3. Segue da Definição 1, de coeficiente binomial, que

$$\binom{n}{0}=\frac{n!}{0!(n-0)!}=\frac{n!}{1\cdot n!}=1$$

$$\binom{n}{n}=\frac{n!}{n!(n-n)!}=\frac{n!}{n!\cdot 1}=1$$

mais ainda, é interessante notar que

$$\binom{n}{1}=\frac{n!}{1!(n-1)!}=\frac{n\cdot(n-1)!}{1\cdot(n-1)!}=n,$$

$$\binom{n}{n-1}=\frac{n!}{(n-1)!(n-[n-1])!}=\frac{n!}{(n-1)!1!}=\frac{n\cdot(n-1)!}{(n-1)!1!}=n.$$

Das considerações acima, podemos agora provar o Teorema do binômio de Newton.

Teorema 1. (Binômio de Newton) Seja $n\in\mathbb{N}$ e a e b números reais. Sejam $n\in\mathbb{N}$ e a e b números reais. Então

$$(a+b)^n=\binom{n}{0}a^nb^0+\binom{n}{1}a^{n-1}b^1+\cdots+\binom{n}{k}a^{n-k}b^k+\cdots+\binom{n}{n-1}a^1b^{n-1}+\binom{n}{n}a^0b^n.$$

Demonstração. Demonstraremos o teorema por indução matemática e usaremos a notação $(a+b)^n=\sum_{k=0}^{\infty}\binom{n}{k}a^{n-k}b^k$.

Verifiquemos a validade da igualdade para $n=1$.

$$\sum_{k=0}^{1}\binom{1}{k}a^{1-k}b^k=\binom{1}{0}a^1b^0+\binom{1}{1}a^0b^1=a+b=(a+b)^1.$$

Logo, a igualdade vale para $n=1$.

Suponha agora que $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k$ para algum $n \in \mathbb{N}$. Mostremos que a igualdade vale para $n+1$. Por hipótese, temos que

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k$$

Multiplicando ambos os membros por $(a+b)$, temos que

$$\begin{aligned}
(a+b)^{n+1} &= \left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k\right) \cdot (a+b) \\
&= a \cdot \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k + b \cdot \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n-k+1}b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^{k+1} \\
&= \binom{n}{0} a^{n+1}b^0 + \sum_{k=1}^{n} \binom{n}{k} a^{n-k+1}b^k + \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k}b^{k+1} + \binom{n}{n} a^0 b^{n+1} \\
&= a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n-k+1}b^k + \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k}b^{k+1} + b^{n+1} \\
&= a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n-k+1}b^k + \sum_{k=1}^{n} \binom{n}{k-1} a^{n-k+1}b^k \\
&= a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k} a^{n-k+1}b^k + \binom{n}{k-1} a^{n-k+1}b^k\right] \\
&= a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1}\right] a^{n-k+1}b^k.
\end{aligned}$$

Logo, pela Propriedade 4, (b) temos que

$$(a+b)^{n+1} = 1 \cdot a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^{n-k+1}b^k + 1 \cdot b^{n+1}$$

Como $a^{n+1} = \binom{n+1}{0} a^{n-0+1}b^0$ e $b^{n+1} = \binom{n+1}{n+1} a^{n-[n+1]+1}b^{n+1}$ temos que

$$(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^{(n+1)-k}b^k,$$

o que completa nossa demonstração. □

Observação 4. Se assumirmos a existência do conjunto dos números racionais para $b \neq 0$ basta substituir x por $\dfrac{b}{a}$ na expansão $(1+x)^n$ e multiplicar os dois lados por a^n que obtemos outra prova para o Teorema do Binômio de Newton.

Usualmente escrevemos os coeficientes binomiais $\binom{n}{k}$, acrescentando $\binom{0}{0} = 1$ ordenados no chamado triângulo de Pascal, cuja n-ésima linha fornece os coeficientes no desenvolvimento de $(a+b)^n$ para cada $n \in N_0$.

$$\binom{0}{0}$$
$$\binom{1}{0} \quad \binom{1}{1}$$
$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$
$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$
$$\cdots\cdots\cdots\cdots$$
$$\binom{n}{0} \quad \binom{n}{1} \quad \cdots \quad \binom{n}{k-1} \quad \binom{n}{k} \quad \cdots \quad \binom{n}{n-1} \quad \binom{n}{n}$$
$$\binom{n+1}{0} \quad \binom{n+1}{1} \quad \cdots \quad \binom{n+1}{k} \quad \cdots \quad \binom{n+1}{n} \quad \binom{n+1}{n+1}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

Note que aqui conseguimos visualizar a Propriedade 4 b), em que o termo $\binom{n+1}{k}$ da $(n+1)$-ésima linha do Triângulo de Pascal é obtido a partir da soma dos termos vizinhos $\binom{n}{k-1}$ e $\binom{n}{k}$ da linha anterior. Como consequência desta propriedade podemos mostrar facilmente o seguinte resultado.

Proposição 5. Os coeficientes binomiais são números inteiros.

Demonstração. Mostremos este resultado por indução sobre $n \in \mathbb{N}$.

Os coeficientes binomiais são definidos em $\mathbb{N}$, isto é, $n \geqslant 1$.

Para $n = 1$ temos que

$$\binom{1}{k} = \frac{1!}{k!(1-k)!} = 1 \in \mathbb{Z}$$

para $0 \leqslant K \leqslant 1$ (isto é, $k = 0$ e $k = 1$).

Suponhamos agora que

$$\binom{n}{k} \in \mathbb{Z} \text{ para todo } 0 \leqslant k \leqslant n.$$

Seja $0 \leqslant k \leqslant n$. Pela Propriedade ou pelo Triângulo de Pascal sabemos que $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$. E, dessa forma, como hipótese de indução $\binom{n}{k-1} \in \mathbb{Z}$ e $\binom{n}{k} \in \mathbb{Z}$ para $0 \leqslant k < n+1$, concluímos que $\binom{n+1}{k}$ é inteiro e então os coeficientes binomiais são números inteiros. □

Definição 2. Para todo $n \in \mathbb{N}$ e todo $m \in \mathbb{N}_0$, denotamos a soma das n primeiras m-ésimas potências por

$$S_n(m) = \sum_{k=1}^{n} k^m = 1^m + 2^m + 3^m + \cdots + n^m.$$

Exemplo 5. Temos que

$$S_n(0) = 1^0 + 2^0 + 3^0 + \cdots + n^0 = 1 + 1 + 1 + \cdots + 1 = n.$$

Além disso

$$\begin{aligned} S_n(1) &= 1^1 + 2^1 + 3^1 + \cdots + n^1 \text{ é a soma dos n primeiros números naturais;} \\ S_n(2) &= 1^2 + 2^2 + 3^2 + \cdots + n^2 \text{ é a soma dos n primeiros quadrados perfeitos;} \\ S_n(3) &= 1^3 + 2^3 + 3^3 + \cdots + n^3 \text{ é a soma dos n primeiros cubos perfeitos.} \end{aligned}$$

O teorema a seguir apresentará uma fórmula recursiva que permite calcular $S_n(m)$.

Teorema 2. Para todos os $n, m \in \mathbb{N}$ temos que

$$(m+1) \cdot S_n(m) = (n+1)^{m+1} - 1 - \sum_{k=0}^{m-1} \binom{m+1}{k} S_n(k).$$

Ou seja,

$$(m+1) \cdot S_n(m) = (n+1)^{m+1} - 1 - \binom{m+1}{0} S_n(0) - \binom{m+1}{1} S_n(1) - \ldots - \binom{m+1}{m-1} S_n(m-1).$$

Demonstração. Inicialmente note que pelo Teorema do Binômio de Newton temos que

$$(1+x)^{m+1} = \sum_{k=0}^{m+1} \binom{m+1}{k} x^k.$$

Ou seja, temos que

$$(1+x)^{m+1} = 1 + \binom{m+1}{1} x + \binom{m+1}{2} x^2 + \cdots + \binom{m+1}{k} x^k + \cdots + \binom{m+1}{m} x^m + \binom{m+1}{m+1} x^{m+1}$$

Atribuindo $x = 1, 2, 3, \ldots, n$ temos, respectivamente,

$$\begin{aligned} 2^{m+1} &= 1 + \binom{m+1}{1} 1 + \binom{m+1}{2} 1^2 + \cdots + \binom{m+1}{k} 1^k + \cdots + \binom{m+1}{m} 1^m + 1 \cdot 1^{m+1} \\ 3^{m+1} &= 1 + \binom{m+1}{1} 2 + \binom{m+1}{2} 2^2 + \cdots + \binom{m+1}{k} 2^k + \cdots + \binom{m+1}{m} 2^m + 1 \cdot 2^{m+1} \\ (l+1)^{m+1} &= 1 + \binom{m+1}{1} l + \binom{m+1}{2} l^2 + \cdots + \binom{m+1}{k} l^k + \cdots + \binom{m+1}{m} l^m + 1 \cdot l^{m+1} \\ (n+1)^{m+1} &= 1 + \binom{m+1}{1} n + \binom{m+1}{2} n^2 + \cdots + \binom{m+1}{k} n^k + \cdots + \binom{m+1}{m} n^m + 1 \cdot n^{m+1} \end{aligned}$$

Somando-se verticalmente e cancelando os termos $2^{m+1}, 3^{m+1}, \cdots, n^{m+1}$ temos

$$(n+1)^{m+1} = S_n(0) + \binom{m+1}{1} S_n(1) + \cdots + \binom{m+1}{k} S_n(k) + \cdots + \binom{m+1}{m} S_n(m) + 1$$

Observando a definição de $S_n(k)$, ficamos com

$$(n+1)^{m+1} = S_n(0) + \sum_{k=1}^{m-1} \binom{m+1}{k} S_n(k) + \binom{m+1}{m} S_n(m) + 1.$$

Sabemos que $S_n(0)$ pode ser escrito na forma $\binom{m+1}{0} S_n(0)$ e o incluiremos no somatório, ou seja,

$$(n+1)^{m+1} = \sum_{k=0}^{m-1} \binom{m+1}{k} S_n(k) + \frac{(m+1)!}{m!(m+1-m)!} S_n(m) + 1.$$

Logo,

$$(n+1)^{m+1} = \sum_{k=0}^{m-1} \binom{m+1}{k} S_n(k) + (m+1) \cdot S_n(m) + 1,$$

o que implica que

$$(m+1) \cdot S_n(m) = (n+1)^{m+1} - \sum_{k=0}^{m-1} \binom{m+1}{k} S_n(k) - 1.$$

□

Exemplo 6. Analisemos a seguir os primeiros casos da fórmula obtida no Teorema 2

a) Para $m = 1$, temos:

$$(1+1) \cdot S_n(1) = (n+1)^{1+1} - \sum_{k=0}^{1-1} \binom{1+1}{k} S_n(k) - 1.$$

Ou seja,

$$\begin{aligned} 2 \cdot S_n(1) &= (n+1)^2 - \binom{2}{0} S_n(0) - 1 \\ &= n^2 + 2n + 1 - n - 1 \\ &= n^2 + n = n(n+1), \end{aligned}$$

o que implica que

$$S_n(1) = \frac{n(n+1)}{2},$$

que é a soma dos n primeiros números naturais.

b) Para $m = 2$, temos:

$$(2+1) \cdot S_n(2) = (n+1)^{2+1} - \sum_{k=0}^{2-1} \binom{2+1}{k} S_n(k) - 1.$$

Ou seja,

$$\begin{aligned}
3\cdot S_n(2) &= (n+1)^3 - \sum_{n+1}^{3} - \sum_{k=0}^{1}\binom{3}{k}S_n(k) - 1 \\
&= (n+1)^3 - \left[\binom{3}{0}S_n(0) + \binom{3}{1}S_n(1)\right] - 1 \\
&= (n+1)^3 - \left[n + 3\left[\frac{n(n+1)}{2}\right]\right] - 1 \\
&= (n+1)^3 - n - \frac{3n(n+1)}{2} - 1 \\
&= (n+1)^3 - (n+1) - \frac{3n(n+1)}{2} \\
&= (n+1)\left[(n+1)^2 - 1 - \frac{3n}{2}\right] \\
&= (n+1)\left[\frac{2n^2+n}{2}\right] = \frac{(n+1)n(2n+1)}{2},
\end{aligned}$$

o que implica que

$$S_n(2) = \frac{n(n+1)(2n+1)}{6}.$$

c) Para $m = 3$, temos:

$$(3+1)\cdot S_n(3) = (n+1)^{3+1} - \sum_{k=0}^{3-1}\binom{3+1}{k}S_n(k) - 1.$$

Ou seja,

$$\begin{aligned}
4\cdot S_n(3) &= (n+1)^4 - \sum_{k=0}^{2}\binom{4}{k}S_n(k) - 1 \\
&= (n+1)^4 - \left[\binom{4}{0}S_n(0) + \binom{4}{1}S_n(1) + \binom{4}{2}S_n(2)\right] - 1 \\
&= (n+1)^4 - \left[n + \frac{4n(n+1)}{2} + \frac{6n(n+1)(2n+1)}{6}\right] - 1 \\
&= (n+1)^4 - n - 2n(n+1) - 1 \\
&= (n+1)^4 - (n+1) - 2n(n+1) - n(n+1)(2n+1) \\
&= (n+1)\left[(n+1)^3 - 1 - 2n - n(2n+1)\right] \\
&= (n+1)(n^3 + 3n^2 + 3n + 1 - 1 - 2n - 2n^2 - n) \\
&= (n+1)(n^3 + n^2) = (n+1)n^2(n+1) = (n+1)^2n^2,
\end{aligned}$$

o que implica que

$$S_n(3) = \frac{n^2(n+1)^2}{4}.$$

Observação 5. Ao compararmos os casos em que $m = 1$ e $m = 3$ no Exemplo acima vemos que

$$S_n(3) = (S_n(1))^2$$

o que representa a seguinte relação interessante

$$(1+2+3+\cdot+n)^2 = 1^3+2^3+3^3+\cdot+n^3,\ \forall\, n \in \mathbb{N}.$$

Uma fórmula para $S_n(m)$ sem o uso das somas anteriores pode ser obtida a partir do determinante de uma matriz $(m+1)\times(m+1)$. A seguir apresentaremos um resultado com esta fórmula.

Teorema 3. Para todo $n \in \mathbb{N}$ e $m \in \mathbb{N}_0$, temos

$$S_n(m) = \frac{1}{(m+1)!}\cdot \begin{vmatrix} \binom{1}{0} & 0 & 0 & \cdots & 0 & 0 & (n+1)^1-1 \\ \binom{2}{0} & \binom{2}{1} & 0 & \cdots & 0 & 0 & (n+1)^2-1 \\ \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \cdots & 0 & 0 & (n+1)^3-1 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ \binom{m}{0} & \binom{m}{1} & \binom{m}{2} & \cdots & \binom{m}{m-2} & \binom{m}{m-1} & (n+1)^m-1 \\ \binom{m+1}{0} & \binom{m+1}{1} & \binom{m+1}{2} & \cdots & \binom{m+1}{m-2} & \binom{m+1}{m-1} & (n+1)^{m+1}-1 \end{vmatrix}$$

Demonstração. Da fórmula obtida no Teorema 2 temos que

$$(m+1)\cdot S_n(m) = (n+1)^{m+1} - 1 - \sum_{k=0}^{m-1}\binom{m+1}{k} S_n(k).$$

Como $(m+1) = \binom{m+1}{m}$, escreveremos a equação acima da seguinte maneira

$$\binom{m+1}{m}\cdot S_n(m) + \sum_{k=0}^{m-1}\binom{m+1}{k} S_n(k) = (n+1)^{m+1} - 1.$$

Incluindo $\binom{m+1}{n}\cdot S_n(m)$ no somatório, temos

$$\sum_{k=0}^{m}\binom{m+1}{k} S_n(k) = (n+1)^{m+1} - 1.$$

Fazendo uma mudança de variável, $m = l$ reescreveremos a igualdade anterior como

$$\sum_{k=0}^{l}\binom{l+1}{k} S_n(k) = (n+1)^{l+1} - 1.$$

Atribuindo valores para l, ou seja, tomando $l = 0,1,2,3,...,m$ obtemos o seguinte sistema de $(m+1)$ equações lineares com $(m+1)$ incógnitas, sendo elas $S_n(0), S_n(1), S_n(2), \cdots, S_n(m)$

$$\begin{cases} \binom{1}{0}S_n(0) = (n+1)^1 - 1 \\ \binom{2}{0}S_n(0) + \binom{2}{1}S_n(1) = (n+1)^2 - 1 \\ \binom{3}{0}S_n(0) + \binom{3}{1}S_n(1) + \binom{3}{2}S_n(2) = (n+1)^3 - 1 \\ \vdots \\ \binom{m}{0}S_n(0) + \binom{m}{1}S_n(1) + \cdots + \binom{m}{m-1}S_n(m-1) = (n+1)^m - 1 \\ \binom{m+1}{0}S_n(0) + \binom{m+1}{1}S_n(1) + \cdots + \binom{m+1}{m-1}S_n(m-1) + \binom{m+1}{m}S_n(m) = (n+1)^{m+1} - 1 \end{cases}$$

Para resolver esse sistema calcularemos o determinante da matriz dos coeficientes. Chamaremos esse determinante por D. Ou seja,

$$D=\begin{vmatrix} \binom{1}{0} & 0 & 0 & \cdots & 0 & 0 \\ \binom{2}{0} & \binom{2}{1} & 0 & \cdots & 0 & 0 \\ \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ \binom{m}{0} & \binom{m}{1} & \binom{m}{2} & \cdots & \binom{m}{m-1} & 0 \\ \binom{m+1}{0} & \binom{m+1}{1} & \binom{m+1}{2} & \cdots & \binom{m+1}{m-1} & \binom{m+1}{m} \end{vmatrix}$$

Podemos notar que essa matriz é a do tipo triangular e dessa forma seu determinante é dado pelo produto dos elementos da diagonal principal. Logo

$$D=\binom{1}{0}\cdot\binom{2}{1}\cdot\binom{3}{2}\cdot\cdots\cdot\binom{m}{m-1}\cdot\binom{m+1}{m}=$$

$$=\frac{1!}{0!(1-0)!}\cdot\frac{2!}{1!(2-1)!}\cdot\frac{3!}{2!(3-2)!}\cdot\cdots\cdot\frac{m!}{(m-1)!(m-m+1)!}\cdot\frac{(m+1)!}{m!(m+1-m)!}=(m+1)!$$

Portanto, utilizando a Regra de Cramer determinamos a incógnita $S_n(m)$, da seguinte forma

$$S_n(m)=\frac{1}{(m+1)!}\cdot\begin{pmatrix} \binom{1}{0} & 0 & 0 & \cdots & 0 & 0 & (n+1)^1-1 \\ \binom{2}{0} & \binom{2}{1} & 0 & \cdots & 0 & 0 & (n+1)^2-1 \\ \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \cdots & 0 & 0 & (n+1)^3-1 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ \binom{m}{0} & \binom{m}{1} & \binom{m}{2} & \cdots & \binom{m}{m-2} & \binom{m}{m-1} & (n+1)^m-1 \\ \binom{m+1}{0} & \binom{m+1}{1} & \binom{m+1}{2} & \cdots & \binom{m+1}{m-2} & \binom{m+1}{m-1} & (n+1)^{m+1}-1 \end{pmatrix}$$

□

2.3 Números triangulares e quadrados perfeitos

Definição 3. Para todo $m\in\mathbb{N}$ definimos $t_m=\dfrac{m(m+1)}{2}$, e dizemos que t_m é o m-ésimo termo triangular.

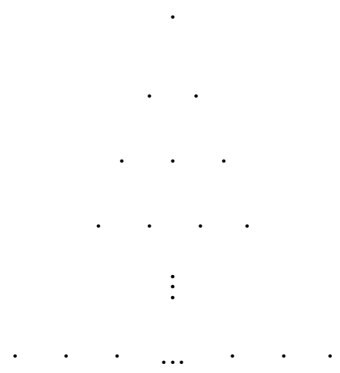
Observação 6. Note que para todo $m\in\mathbb{N}$ temos

$$S_m(1)=1+2+3+\cdots+m=\binom{m+1}{2}=\frac{(m+1)!}{2!(m-1)!}=\frac{(m+1)\cdot m\cdot(m-1)!}{2\cdot(m-1)!}=\frac{m\cdot(m+1)}{2}=t_m$$

tal como $t_{m+1}=1+2+3+\cdots+m+(m+1)=t_m+(m+1)$ A sequência dos números triangulares é

$$(t_m)_{m\in\mathbb{N}}=\left((1,3,6,10,...,\frac{m(m+1)}{2},...\right).$$

O uso do termo "número triangular"para os números desta sequência é motivado pelo seguinte triângulo equilátero de lados m o qual contém exatamente t_m pontos



A seguinte propriedade é um resultado clássico entre os números triangulares e os números naturais.

Proposição 6. Seja $n \in \mathbb{N}$. Então n é um número triangular, se e somente se, $8n+1$ é um quadrado perfeito.

Demonstração. Suponhamos que n seja um número triangular, ou seja, $t_m = n$, para algum $m \in \mathbb{N}$. Assim, $8n+1 = 8t_m + 1 = 8 \cdot \dfrac{m(m+1)}{2} + 1 = 4m^2 + 4m + 1 = (2m+1)^2$ que é um quadrado perfeito.

Seja agora $n \in \mathbb{N}$ tal que $8n+1$ seja um quadrado perfeito,ou seja, $8n+1 = k^2$ para algum $k \in \mathbb{N}$. Então k^2 é ímpar e dessa forma k é ímpar com $k \geqslant 3$. Logo, temos que $k-1$ é par assim, $\dfrac{k-1}{2} \in \mathbb{N}$. Considerando o m-ésimo número triangular com $m = \dfrac{k-1}{2}$, temos

$$\begin{aligned} t_m = t_{\frac{k-1}{2}} &= \frac{\frac{k-1}{2}\left(\frac{k-1}{2}+1\right)}{2} = \left[\frac{k^2-2k+1}{4} + \frac{k-1}{2}\right] \cdot \frac{1}{2} \\ &= \frac{k^2-2k+1+2k-2}{4} \cdot \frac{1}{2} = \frac{k^2-1}{4} \cdot \frac{1}{2} = \frac{k^2-1}{8}. \end{aligned}$$

Logo, como $8n+1 = k^2$ temos $n = \dfrac{k^2-1}{8}$,e $t_m = n$ para $m = \dfrac{k-1}{2}$. Ou seja, n é um número triangular. □

Para os quadrados perfeitos ainda valem as propriedades na seguinte Proposição.

Proposição 7. Seja $n \in \mathbb{N}$ um quadrado perfeito, então valem as seguintes propriedades.

a) Se n é par, então n é divisível por 4.

b) Se n é ímpar, então n é da forma $8k+1$, com $k \in \mathbb{N}$, isto é, n deixa o resto 1 quando dividido por 8.

Demonstração. (a) Suponha que n é par e que $n = m^2$, com $m \in \mathbb{N}$. Como m^2 é par, então m é par. Logo $m = 2k$ e $n = m^2 = (2k)^2 = 4k^2$, que é divisível por 4.

(b) Suponha que n é ímpar e que $n = m^2$, com $m \in \mathbb{N}$. Como m^2 é ímpar, então m é ímpar. Então $m = 2l - 1$ e $n = m^2 = (2l-1)^2 = 4l^2 - 4l + 1 = 4l(l-1) + 1$. Sabemos que $(l-1)$ e l são números consecutivos e dessa forma, um deles é par e faz com que o produto $l(l-1) = 2k$. Então

$$n = 4 \cdot 2k + 1 = 8k + 1.$$

□

Observação 7. Se $n \in \mathbb{N}$ é um quadrado perfeito ímpar, então podemos obter um número triangular a partir de n. De fato, pela Proposição 7 $n = 8k + 1$ para algum $k \in \mathbb{N}_0$. Logo, pela Proposição 4 k é um número triangular.

Exemplo 7. Na sequência dos números $11, 111, 1111, ..., 11111...111, ...$ não aparece nenhum quadrado perfeito.

De fato temos que $11 = 8 \cdot 1 + 3$ que não é da forma $8k + 1$, e assim não é um quadrado perfeito, pela proposição 7.

Analisando o número $n = 111...111$ temos $n = 111...1000 + 111$. Podemos notar pelo critério de divisibilidade por 8 que a primeira parcela é um número múltiplo de oito, podendo ser escrita da forma $8l$, $l \in \mathbb{N}$. Já a segunda parcela, pode ser escrita da forma $8 \cdot 13 + 7$, e dessa forma:

$$n = 111...1000 + 111 = 8l + 8 \cdot 13 + 7 = 8(l + 13) + 7 = 8k + 7.$$

Portanto, podemos dizer que nenhum número na sequência é da forma $8k + 1$, condição necessária para ser um quadrado perfeito.

Além dos próprios quadrados perfeitos existem muitos números naturais que podem ser escritos como diferença de dois quadrados, $n = x^2 - y^2$, em que $x, y \in \mathbb{N}_0$. Por outro lado, os números 2 e 6, por exemplo não gozam dessa propriedade.Os números que são diferença de dois quadrados são caracterizados no seguinte resultado.

Proposição 8. Seja $n \in \mathbb{N}$. Então, $n = x^2 - y^2$, em que $x, y \in \mathbb{N}_0$ se, e somente se,

$$n \notin \{2, 6, 10, 14, ..., 4k + 2, ...\}.$$

Ou seja, n é a diferença de dois quadrados, se e somente se n é ímpar ou divisível por 4.

Demonstração. Suponha que $n = x^2 - y^2$, onde $x, y \in \mathbb{N}_0$. Devemos mostrar que $n \notin \{2, 6, 10, ...\}$. Podemos supor ainda que n é par, visto que se n for ímpar ele já não pertence ao conjunto. Logo devemos ter que x e y, são ambos pares ou ambos ímpares. Sendo ambos pares, ou seja, $x = 2k$ e $y = 2l$, temos que $n = x^2 - y^2 = (2k)^2 - (2l)^2 = 4k^2 = 4l^2 = 4(k^2 - l^2)$. Portanto, como n

é múltiplo de 4, $n \notin \{2,6,10,\cdots\}$. Sendo ambos ímpares, ou seja, $x = 2k-1$ e $y = 2l-1$, temos $n = x^2 - y^2 = (2k-1)^2 - (2l-1)^2 = (4k^2 - 4k + 1) - (4l^2 - 4l + 1) = 4(k^2 - k - l^2 + l)$. Portanto, como n é múltiplo de 4, $n \notin \{2,6,10,...\}$.

Suponha agora que $n \in \{2,6,10,...\}$, ou seja, n é ímpar ou divisível por 4. Se n é ímpar, $n \pm 1$ é par e portanto divisíveis por 2, ou seja, $\frac{n \pm 1}{2} \in \mathbb{N}_0$. Temos ainda que n pode ser obtido a partir de uma diferença de dois quadrados. De fato, note que

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

Logo $n = x^2 - y^2$, com $x = \frac{n+1}{2} \in \mathbb{N}_0$ e $y = \frac{n-1}{2} \in \mathbb{N}_0$.

Se $n = 4k$. também podemos obter n a partir de uma diferença de quadrados. Veja $n = 4k = k^2 + 2k + 1 - k^2 + 2k - 1 = (k^2 + 2k + 1) - (k^2 - 2k + 1) = (k+1)^2 - (k-1)^2$.

Portanto, como $k = \frac{n}{4}$, temos:

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

Concluímos assim a demonstração □

Temos como curiosidade que pensando na subdivisão do conjunto $\mathbb{N}$ nos quatro subconjuntos a seguir:

$$\mathbb{N} = \{4,8,12,...\} \cup \{1,5,9,13,...\} \cup \{2,6,10,14,...\} \cup \{3,7,11,15,...\}$$

pode-se verificar que dentre esses não são diferença de dois quadrados os números do conjunto $\{2,6,10,14,...\}$, que significa que 75% dos números naturais são diferença de dois quadrados.

CAPÍTULO

3

TEORIA DAS DIVISIBILIDADES DOS NÚMEROS INTEIROS

Nem sempre é possível a divisão de um número inteiro por outro. Logo, expressamos essa possibilidade através da relação de divisibilidade. Quando não existir uma relação de divisibilidade entre dois números inteiro veremos que, ainda assim, será possível efetuar uma "divisão com resto pequeno", chamada divisão euclidiana. O fato de sempre ser possível efetuar tal divisão é responsável por diversas propriedades dos inteiros, das quais veremos algumas neste capítulo.

3.1 O algoritmo geral de divisão

Proposição 9. (O Algoritmo de Divisão) Sejam $a, b \in \mathbb{Z}$ com $b > 0$. Então existem dois únicos números inteiros q, r tais que

$$a = qb + r \text{ com } 0 \leqslant r < b.$$

O número q chama-se o quociente e r o menor resto não-negativo na divisão de a por b.

Demonstração. Provemos inicialmente a existência de q e r. Dados $a, b \in \mathbb{Z}$ com $b > 0$, considere o conjunto

$$S = \{a - bx | x \in \mathbb{Z}, a - bx \geqslant 0\}.$$

Temos que $S \subset \mathbb{N}_0$. Além disso, para $x = -|a|$

$$a - bx = a - b \cdot (-|a|) = a + b \cdot |a| \geqslant a + |a| \geqslant 0$$

já que $b \geqslant 1$. Dessa forma, $S \neq \emptyset$.

Pelo princípio da indução temos que existe um elemento mínimo, isto é, $r \leqslant y$, para todo $y \in S$. Como $r \in S$, existe $x = q, q \in \mathbb{Z}$, tal que $r = a - bq$, ou seja $a = bq + r$.

Provemos que $0 \leqslant r < b$. Como $r \in S$ e $S \subset \mathbb{N}_0$ temos que $r \geqslant 0$. Agora, para mostrar que $r < b$ vamos supor $r \geqslant b$. Então, $r = b + s$ com $0 \leqslant s < r$. Logo, $a - bq = b + s$, o que implica que $s = a - bq - b \geqslant 0$. Ou seja, $s = a - b(q+1) \in S$ e $s < r$ o que contradiz o fato de r ser o menor elemento de S.

Para a unicidade suponhamos que q, r, q' e r' são inteiros tais que

$$a = bq + r = bq' + r' \text{ com } 0 \leqslant r < b \text{ e } 0 \leqslant r' < b.$$

Então $r' - r = bq - bq' = b(q - q')$. Das condições $0 \leqslant r < b$ e $0 \leqslant r' < b$ apresentadas acima, temos que $0 \leqslant r' < b$ e $-b < -r \leqslant 0$. Logo $-b < r' - r < b$ e da desigualdade modular temos $|r' - r| < b$. O que implica que $b \geqslant b|q - q'|$ pois $B \leqslant 1$. Se $q \neq q'$ a última desigualdade é uma contradição. Logo devemos ter $q = q'$ e, portanto, $r = r'$. □

Exemplo 8. Para $a = 100$ e $b = 7$, temos $q = 14$ e $r = 2$, pois $100 = 7 \cdot 14 + 2$.

Para $a = -100$ e $b = 7$, temos $q = -15$ e $r = 5$, pois $-100 = 7 \cdot (-15) + 5$.

Teorema 4. (Algoritmo da divisão) Para quaisquer números $a, b \in \mathbb{Z}$ com $b \neq 0$ existem dois únicos números $q, r \in \mathbb{Z}$, tais que

$$a = bq + r \text{ e } 0 \leqslant r < |b|.$$

Demonstração. Temos $|b| > 0$. Da Proposição 9 existem únicos $q', r \in \mathbb{Z}$ com $a = |b|q' - r$, com $0 \leq r \leq |b|$. Se $b > 0$, temos $|b| = b$ e podemos considerar $q = q'$ junto com r. Se $b < 0$, temos $|b| = -b$ e podemos considerar $q = -q'$ junto com r, obtendo $a = |b|q' + r \Rightarrow a = (-b)q' + r \Rightarrow a = b(-q') + r \Rightarrow a = bq + r$. □

Exemplo 9. Para $a = 100$ e $b = -7$, temos $q = -14$ e $r = 2$, pois $100 = (-7) \cdot (-14) + 2$.

Para $a = -100$ e $b = -7$, temos $q = 15$ e $r = 5$, pois $-100 = (-7) \cdot 15 + 5$.

Observação 8. Dos resultados acima podemos notar as seguintes considerações.

a) Se $b = 2$ temos que para qualquer $a \in \mathbb{Z}$ existe um único $q \in \mathbb{Z}$ tal que $a = 2q$ ou $a = 2q + 1$ e, consequentemente, que

$$\mathbb{Z} = \{2q | q \in \mathbb{Z}\} \cup \{2q + 1 | q \in \mathbb{Z}\}$$

tal que

$$\{2q | q \in \mathbb{Z}\} \cap \{2q + 1 | q \in \mathbb{Z}\} = \emptyset$$

isto é, temos uma decomposição do conjunto $\mathbb{Z}$ em dois subconjuntos disjuntos, os inteiros pares e os inteiros ímpares.

b) De forma semelhante, Se $b = 3$, temos que para qualquer $a \in \mathbb{Z}$ existe um único $q \in \mathbb{Z}$ com $a = 3q$ ou $a = 3q+1$ ou $a = 3q+2$ e, consequentemente,

$$\mathbb{Z} = \{3q|q \in \mathbb{Z}\} \cup \{3q+1|q \in \mathbb{Z}\} \cup \{3q+2|q \in \mathbb{Z}\}$$

é uma decomposição de $\mathbb{Z}$ em três conjuntos disjuntos.

c) Em geral, para $b = n \in \mathbb{N}$ obtemos a união disjunta

$$\mathbb{Z} = \{nq|q \in \mathbb{Z}\} \cup \{nq+1|q \in \mathbb{Z}\} \cup \{nq+2|q \in \mathbb{Z}\} \cup \cdots \cup \{nq+(n-1)|q \in \mathbb{Z}\}$$

que chamamos de classes de resto módulo n, as quais estudaremos posteriormente.

Definição 4. Dizemos que um inteiro b é divisível por um inteiro a ou que a divide b se existe $q \in \mathbb{Z}$ tal que $b = a \cdot q$.

Notação: Escrevemos $a|b$ se a divide b e $a \nmid b$ se isso não ocorre. Exemplos, temos que $3|-12$, $5|15$ e $-7|21$. Além disso $1|b$ para todo $b \in \mathbb{Z}$ e $a|0$ para todo $a \in \mathbb{Z}$.

Proposição 10. Para todos os números $a, b, c, d \in \mathbb{Z}$ valem as seguintes propriedades.

a) $a|0$, $1|b$ e $a|a$.

b) $a|1 \Leftrightarrow a = \pm 1$ e $0|b \Leftrightarrow b = 0$.

c) Se $a|b$ e $c|d$ então $ac|bd$.

d) Se $a|b$ e $b|c$ então $a|c$.

e) $a|b$ e $b|a \Leftrightarrow a = \pm b$.

f) Se $a|b$ e $b \neq 0$, então $|a| \leq |b|$.

g) Se $a|b \pm c$, então $a|b \Leftrightarrow a|c$.

h) Se $a|b$ e $a|c$ então $a|bx+cy \forall x, y \in \mathbb{Z}$.

Demonstração. (a) De fato, temos que $0 = a \cdot 0$, $b = 1 \cdot b$ e $a = a \cdot 1$.

(b) ($\Rightarrow$) Se $a|1$, então $1 = a \cdot q, q \in \mathbb{Z}$. Mas um produto de dois números inteiros resultando em 1, somente dá-se ambos forem iguais a 1 ou -1. Portanto, $a = q = 1$ ou $a = q = -1$.

($\Leftarrow$) Se $a = 1$, então podemos escrever que $a \cdot 1 = 1$ e portanto, $a|1$. Se $a = -1$, então podemos escrever que $a \cdot (-1) = 1$ e portanto, $a|1$.

($\Rightarrow$)Se $0|b$, então $b = 0 \cdot q = 0$, portanto $b = 0$. ($\Leftrightarrow$) Se $b = 0$, então $b = 0 \cdot q$ ou $b = a \cdot 0$ e portanto $0|b$.

(c) De fato, $a|b \Rightarrow b = a \cdot q_1$, $c|d \Rightarrow d = c \cdot q_2$, q_1 e $q_2 \in \mathbb{Z}$. Então $bd = a \cdot q_1 \cdot c \cdot q_2 = ac \cdot q_1 \cdot q_2 = ac \cdot q$, $q \in \mathbb{Z}$. O que implica que $ac|bd$.

(d) De fato, $a|b \Rightarrow b = a \cdot q_1$ e $b|c \Rightarrow c = b \cdot q_2$, q_1, $q_2 \in \mathbb{Z}$. Então $c = a \cdot q_1 \cdot q_2 \Rightarrow c = a \cdot q, q \in \mathbb{Z}$. O que implica que $a|c$.

(e) Se $a|b$ e $b|a$, então $b = a \cdot q_1$ e $a = b \cdot q_2$, q_1 , $q_2 \in \mathbb{Z}$. Dessa forma, $a = a \cdot q_1 \cdot q_2$, o que implica que $q_1 \cdot q_2 = 1$ e, portanto, $q_1 = q_2 = 1$ ou $q_1 = q_2 = -1$, fazendo com que $a = b$ ou $a = -b$.

Por outro lado se $a = b$, então $b = a \cdot 1$ e $a = b \cdot 1$ e dessa forma, $a|b$ e $b|a$. Se $a = -b$, então $b = a \cdot (-1)$, $a = b \cdot (-1)$ e dessa forma, $a|b$ e $b|a$.

(f) De fato, $a|b \Rightarrow b = a \cdot q$, $q \in \mathbb{Z} \Rightarrow |b| = |aq| = |a||q| \leqslant |a| \Rightarrow |a| \leqslant |b|$.

(g) Suponhamos que $a|b+c$. Então existe $q_1 \in \mathbb{Z}$ tal que $b+c = a \cdot q_1$. Agora se $a|b$, então, existe $q_2 \in \mathbb{Z}$ tal que $b = a \cdot q_2$. Juntando as duas últimas igualdades temos que $aq_2 + c = aq_1$ e, portanto, $c = a(q_1 - q_2)$. Logo $a|c$. A implicação contrária é análoga. Por outro lado, se $a|b-c$ e $a|b$, pelo caso anterior temos que $a|(-c)$, o que implica que $a|c$.

(h) De fato, $a|b \Rightarrow b = a \cdot q_1$ e $a|c \Rightarrow c = a \cdot q_2$, q_1 e $q_2 \in \mathbb{Z}$. Logo $bx + cy = a \cdot q_1 x + a \cdot q_2 y = a(q_1 x + q_2 y) = aq_3$, $q_3 \in \mathbb{Z}$, e portanto, $a|bx + cy$. □

3.2 Máximo divisor comum de dois números

Definição 5. Sejam a, b $\in \mathbb{Z}$ dois números, pelo menos um deles diferente de zero. O máximo divisor comum entre a e b é o número natural $d = \text{mdc}(a,b)$ definido pelas duas propriedades seguintes

a) $d|a$ e $d|b$, isto é, d é divisor comum de a e b.

b) Se algum $c \in \mathbb{N}$ dividir ambos a e b, então $c|d$.

Exemplo 10. É fácil ver que $\text{mdc}(12,18) = 6$, pois os divisores de 12 e 18 são ± 1, ± 2, ± 3 e ± 6.

O próximo Lema prova a existência do máximo divisor comum entre dois inteiros não negativos. Este Lema é muito importante em aplicações e será essencial nas provas dos casos particulares do Teorema de Fermat que consideraremos mais adiante.

Lema 1. (Lema de Euclides) Sejam $a,b,n \in \mathbb{Z}$. Se existe $\text{mdc}(a, b-na)$, então

$$\text{mdc}(a,b) = \text{mdc}(a,b-na).$$

Demonstração. Seja $d = \text{mdc}(a,b-na)$. Como $d|a$ e $d|(b-na)$, segue que $d|b$, pois podemos escrever $b = (b-na) + na$. Logo d é um divisor comum de a e b. Suponhamos agora que c

seja divisor comum de a e b. Então c é um divisor comum de a e $b-na$ e, portanto $c|d$. logo $d = \text{mdc}(a,b)$. □

Teorema 5. Sejam $a,b \in \mathbb{Z}$ sendo um deles diferente de zero e seja $d = \text{mdc}(a,b)$. Então existem x_1 , $y_1 \in \mathbb{Z}$ tais que

$$ax_1 + by_1 = d.$$

Demonstração. Consideremos o seguinte conjunto

$$S = \{ax+by|x,y \in \mathbb{Z}, ax+by > 0\}.$$

Seja $a \neq 0$. Fazendo $y = 0$ e se $a > 0, x = 1$ e se $a < 0, x = -1$ temos que $ax+by = a(\pm 1)+b\cdot 0 = |a|$. Logo $ax+by > 0$, o que mostra $S \neq \emptyset$.

Se $a = 0$, por hipótese $b \neq 0$ e $|b| > 0$. Logo para qualquer $x \in \mathbb{Z}$, se $b > 0$, basta tomar $y = 1$ e se $b < 0$, basta tomar $y = -1$ e dessa forma, $ax+by = 0.x+b.(\pm 1) = |b|$. Assim , $ax = by > 0$ o que também mostra $S \neq \emptyset$.Então pelo princípio de indução, existe um $d \in S$ que é mínimo. Como $d \in S$ temos que $d > 0$ e para algum x_1 , $y_1 \in \mathbb{Z}$, temos que $d = ax_1 + by_1$.

Mostraremos a seguir que $d = \text{mdc}(a,b)$.

Dividindo a por d, pelo Algoritmo da divisão geral temos que existem $q,r \in \mathbb{Z}$, tais que $a = q\cdot d + r$ com $0 \leqslant r \leqslant d-1$. Então $r = a - q\cdot d$ e como $d = ax_1 + by_1$, temos

$$r = a - q(ax_1 + by_1) = a(1-qx_1) + b(-qy_1).$$

Se $r > 0$, então $r \in S$ e $r < d$, o que é um absurdo. Portanto temos que $r = 0$ e $a = q.d$, o que implica que $d|a$.

Da mesma forma mostraremos que $d|b$. Dividindo b por d existem $q,r \in \mathbb{Z}$ tais que $b = q\cdot d + r$ com $0 \leqslant r \leqslant d-1$. Então $r = b - q\cdot d = a - q(ax_1 + by_1) = a(1-qx_1) + b(-qy_1)$. Se $r > 0$, $r \in S$ e $r < d$, o que é um absurdo. Logo $r = 0$ e $b = q\cdot d$, o que implica que $d|b$.

Dessa forma, d é divisor comum de a e b e resta mostrar que ele é o máximo divisor comum.

Seja $c \in \mathbb{N}$ tal que $c|a$ e $c|b$. Da Proposição 10 (h) concluímos que $c|ax_1 + by_1$, ou seja $c|d$.Portanto, $d = \text{mdc}(a,b)$. □

Corolário 1. Sejam $a,b \in \mathbb{Z}$, não ambos nulos e seja d=mdc(a,b). Então

$$\{ax+by|x,y \in \mathbb{Z}\} = \{d\cdot z|z \in \mathbb{Z}\},$$

ou seja as combinações lineares inteiras de a e b são exatamente os múltiplos do mdc(a,b).

Demonstração. Seja $T = \{ax+by|x,y \in \mathbb{Z}\}$ e $R = \{d\cdot z|z \in \mathbb{Z}\}$. Pelo Teorema 5 existem $x_1, y_1 \in \mathbb{Z}$ com $d = ax_1 + by_1$. E daí, para todo $z \in \mathbb{Z}$ temos $dz = a(x_1 z) + b(y_1 z)$ e dessa forma, $d\cdot z \in T$

e $R \subset T$. Dado $ax+by \in T$, então do item (h) da Proposição 10 temos $d|ax+by$, pois $d|a$ e $d|b$, o que implica que $ax+by = dz$, para algum $z \in \mathbb{Z}$ e portanto, $ax+by \in R$ e $R \subset T$. Logo $T = R$. □

Definição 6. Dois números $a, b \in \mathbb{Z}$ chamam-se relativamente primos (ou primos entre si) se $\text{mdc}(a,b) = 1$.

Proposição 11. Dois números $a, b \in \mathbb{Z}$ não ambos nulos, são relativamente primos se, e somente se, existem $x_1, y_1 \in \mathbb{Z}$ tais que

$$ax_1 + by_1 = 1.$$

Demonstração. Seja $d = \text{mdc}(a,b)$

Se $d = 1$, pelo Teorema 5 existem $x_1, y_1 \in \mathbb{Z}$ tais que, $ax_1 + by_1 = 1$.

Por outro lado suponha que existem $x_1, y_1 \in \mathbb{Z}$ tais que $ax_1 + by_1 = 1$. Como $d|a$ e $d|b$, pelo item (h) da Proposição 10 $d|ax+by$ e dessa forma $d|1$ e portanto $d = 1$. □

A seguir verificaremos algumas consequências dessa caracterização dos números relativamente primos.

Proposição 12. Sejam $a, b \in \mathbb{Z}$, não ambos nulos e $d = \text{mdc}(a,b)$. Então

$$\text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

Demonstração. Suponha que existam $x, y \in \mathbb{Z}$, tais que $ax+by = d$. Logo $\frac{a}{d}x + \frac{b}{d}y = 1$ e da Proposição 11 concluímos que $\text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. □

Proposição 13. Sejam $a, b, c \in \mathbb{Z}$ tais que $a|c$ e $b|c$.Se $\text{mdc}(a,b) = 1$, então $ab|c$.

Demonstração. Como $a|c$ e $b|c$, temos que $c = a \cdot r$ e $c = b \cdot s$, com r e $s \in \mathbb{Z}$. Como $\text{mdc}(a,b) = 1$, temos pela Proposição 12 que existem $x, y \in \mathbb{Z}$ tais que $ax+by = 1$.

Assim, $c = c \cdot 1 = c.(ax+by) = cax + cby$. Como $c = bs = ar$, temos que

$$c = (bs)ax + (ar)by = ab(sx+ry),$$

com $sx+ry \in \mathbb{Z}$. Logo, $ab|c$. □

Teorema 6. (O lema de Euclides) Sejam $a, b, c \in \mathbb{Z}$ tais que $a|b \cdot c$ e mdc(a,b)=1. Então $a|c$.

Demonstração. Como $a|bc$, temos que $bc = a \cdot r$, com $r \in \mathbb{Z}$. Por outro lado, como $\text{mdc}(a,b) = 1$, temos $ax+by = 1$, com $x, y \in \mathbb{Z}$. Assim,

$$c = c \cdot 1 = c(ax+by) = cax + cby = cax + ary = a(cx+ry),$$

com $cx+ry \in \mathbb{Z}$, o que implica que $a|c$. □

Proposição 14. Sejam $a,b,c \in \mathbb{Z}$ tais que $\text{mdc}(a,b) = \text{mdc}(a,c) = 1$. Então, $\text{mdc}(a,bc) = 1$.

Demonstração. Como $\text{mdc}(a,b) = 1$, temos $ax + by = 1$, com $x,y \in \mathbb{Z}$. Da mesma forma como $\text{mdc}(a,c) = 1$, temos $au + cv = 1$, com $u,v \in \mathbb{Z}$. Assim,

$$1 = 1 \cdot 1 = (ax+by)(au+cv) = ax^2u + axcv + byau + bycx \Rightarrow 1 = a(axu + xcv + byu) + bc(yv),$$

com $axu + xcv + byu$, $yv \in \mathbb{Z}$, o que implica que $\text{mdc}(a,bc) = 1$. □

O conceito de mdc pode ser generalizado.

Definição 7. Um número natural d é o mdc de dados inteiros $a_1, a_2, ..., a_{n-1}, a_n$ e denotamos $d = \text{mdc}(a_1, a_2, \cdots, a_n)$ se valem as seguintes propriedades.

(a) d é um divisor comum de $a_1, a_2, ..., a_n$.

(b) Se c é um divisor comum de $a_1, a_2, ..., a_n$, então $c|d$.

Proposição 15. Dados $a_1, a_2, ..., a_n \in \mathbb{Z}$, não todos nulos, existe o seu mdc e

$$\text{mdc}(a_1, ..., a_n) = \text{mdc}(a_1, ..., a_{n-2}, \text{mdc}(a_{n-1}, a_n)).$$

Demonstração. Provemos por indução sobre $n (n \geqslant 2)$. Para $n = 2$ não há o que provar. Suponhamos que o resultado vale para n. Para provar que o resultado vale para $n+1$ basta mostrar que se d é o mdc de $a_1, \cdots, a_{n-1}, \text{mdc}(a_n, a_{n+1})$, então $d = \text{mdc}(a_1, \cdots, a_n, a_{n+1})$, pois isso também provará sua existência.

Seja $d = \text{mdc}(a_1, ...a_{n-1}, \text{mdc}(a_n, a_{n+1})$. Então, $d|a_1, ...d|a_{n-1}, d|\text{mdc}(a_n, a_{n+1})$, o que implica que $d|a_1, ..., d|a_{n-1}, d|a_n, d|a_{n+1}$.

Além disso se c é um divisor comum de $a_1, ..., a_n, a_{n+1}$, então devemos ter $c|\text{mdc}(a_n, a_{n+1})$. Logo, c é um divisor comum de $a_1, ..., a_{n-1}$ e $\text{mdc}(a_n, a_{n+1})$ e, portanto, $c|d$. □

Definição 8. Dizemos que $a_1, ..., a_n \in \mathbb{Z}$ são primos entre si ou coprimos se $\text{mdc}(a_1, ..., a_n) = 1$.

3.3 Algoritmo euclidiano

A seguir apresentamos uma prova construtiva da existência do mdc dada por Euclides.

Dados dois números $a,b \in \mathbb{Z}$, com $b \neq 0$ consideremos o seguinte processo que se inicia com divisão de a por b.

Colocamos $r_0 = |b|$. Existem $q_1, r_1 \in \mathbb{Z}$, tais que

$$a = bq_1 + r_1, \text{ com } 0 \leqslant r_1 < r_0.$$

Se $r_1 = 0$, o processo pára. Se $r_1 \neq 0$, fazemos a divisão de r_0 por r_1 e dessa forma existem $q_2, r_2 \in \mathbb{Z}$, tais que

$$r_0 = r_1.q_2 + r_2, \text{ com } 0 \leq r_2 < r_1.$$

Se $r_2 = 0$, o processo pára. Se $r_2 \neq 0$, fazemos a divisão de r_1 por r_2 e dessa forma existem $q_2, r_2 \in \mathbb{Z}$, tais que

$$r_1 = r_2.q_3 + r_3, \text{ com } 0 \leqslant r_3 < r_2.$$

Em geral, se o processo já chegou em

$$r_{k-2} = r_{k-1}.q_k + r_k, \text{ com } 0 \leqslant r_k < r_{k-1},$$

o próximo passo é o seguinte.

Se $r_k = 0$, o processo para. Se $r_k \neq 0$, existem $q_{k+1}, r_{k+1} \in \mathbb{Z}$, tais que

$$r_{k-1} = r_k.q_{k+1} + r_{k+1}, \text{ com } 0 \leq r_{k+1} \leqslant r_k.$$

...

Obtemos assim uma sequência decrescente de inteiros não negativos.

$$|b| = r_0 > r_1 > r_2 > ... > r_k > r_{k+1} > ... \geqslant 0$$

Logo, existirá um $n \in \mathbb{N}_0$ tal que $r_n \neq 0$ porém $r_{n+1} = 0$.

Assim, este processo termina da seguinte forma:

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, \text{ com } 0 < r_{n-1} < r_{n-2}$$

$$r_{n-2} = r_{n-1}q_n + r_n, \text{ com } 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1}.$$

O processo descrito chama-se algoritmo Euclidiano para a e b e a partir dele podemos mostrar o seguinte resultado.

Teorema 7. No algoritmo Euclidiano para a e b temos que $r_n = \text{mdc}(a, b)$. Ou seja, o último resto não nulo no algoritmo Euclidiano é o máximo divisor comum entre a e b.

Demonstração. Da última equação do algoritmos Euclidiano vemos que r_n divide todos os restos anteriores. De fato, temos que

$$r_{n-1} = r_n.q_{n+1} \Rightarrow r_n | r_{n-1}$$

$$r_{n-2} = r_{n-1}.q_n + r_n = r_n.q_{n+1}.q_n + r_n = r_n(q_{n+1}.q_n + 1) \Rightarrow r_n | r_{n-2}$$

$r_{n-3} = r_{n-2}.q_{n-1} + r_{n-1} = r_n(q_{n+1}.q_n + 1).q_{n-1} + r_n.q_{n+1} = r_n(q_{n-1}[q_{n+1}.q_n + 1] + q_{n+1}) \Rightarrow r_n | r_{n-3}$

e assim por diante.

Logo $r_n | r_1$ e por consequência $r_n | r_0$. Como $r_0 = |b|$, $r_n \mid |b|$ e portanto $r_n | b$. Além disso, como $a = bq_1 + r_1$ e $r_n | b$, $r_n | r_1$ temos que $r_n | a$. Assim r_n é um divisor comum de a e b.

Assim mostraremos que r_n é o máximo divisor comum de a e b.

A partir da primeira equação do algoritmos Euclidiano, tomando um divisor comum qualquer c de a e b, vemos que c divide todos os restos e em particular $c | r_n$. Logo, $r_n = \text{mdc}(a,b)$. □

Observação 9. O algoritmos euclidiano pode ser sintetizado no seguinte diagrama.

	q_1	q_2	q_3	$\cdots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	$r_n = \text{mdc(a,b)}$
r_1	r_2	r_3	r_4	$\cdots$	r_n		

Exemplo 11. Determine $\text{mdc}(\pm 7519, \pm 8249)$. Vamos nos restringir a valores positivos e tomar $a = 7519$ e $b = 8249$.

O algoritmo Euclidiano nos dá

$$\begin{aligned} 7519 &= 8249 \cdot 0 + 7519 \\ 8249 &= 7519 \cdot 1 + 730 \\ 7519 &= 730 \cdot 10 + 219 \\ 730 &= 219 \cdot 3 + 73 \\ 219 &= 73 \cdot 3 \end{aligned}$$

Concluímos que $\text{mdc}(\pm 7519, \pm 8249) = 73$.

É interessante ilustrar que o algoritmo Euclidiano é útil para se obter soluções $x, y \in \mathbb{Z}$ com $ax + by = \text{mdc}(a,b)$.

A partir da penúltima equação do algoritmo, temos:
$73 = 730 - 219 \cdot 3 = 730 - (7519 - 730 \cdot 10) \cdot 3 = 730 - 7519 \cdot 3 + 730 \cdot 30 = 31 \cdot 730 - 3 \cdot 7519 = 31(8249 - 7519 \cdot 1) - 3 \cdot 7519 = 31 \cdot 8249 - 34 \cdot 7519$, ou seja $73 = -34 \cdot 7519 + 31 \cdot 8249$. E portanto $x = -34$ e $y = 31$.

3.4 O mínimo múltiplo comum

Definição 9. Sejam $a,b \in \mathbb{Z}$ dois números ambos não-nulos. O mínimo múltiplo comum entre a e b é o número natural $m = \text{mmc}(a,b)$ definido pelas duas propriedades a seguir.

a) $a|m$ e $b|m$, o que quer dizer que m é múltiplo comum de a e b.

b) Se $a|c$ e $b|c$ para algum $c \in \mathbb{N}$, então $m|c$.

Exemplo 12. Para $a = 6$ e $b = -8$ temos os múltiplos comuns destes números são $\pm 24; \pm 48; \pm 72; ....$ Entretanto $m =$mmc$(6,-8) = 24$.

Proposição 16. Sejam $a,b \in \mathbb{Z}$, com $a,b \neq 0$, d=mdc(a,b) e m=mmc(a,b). Então, $m \cdot d = |a \cdot b|$.

Demonstração. Seja $m' = \dfrac{|a \cdot b|}{d}$. Como $d = \text{mdc}(a,b)$ sabemos que existe $r,t \in \mathbb{Z}$ tais que $dr = a$ e $dt = b$.

Logo, $m' = \dfrac{|dr||b|}{d} = \dfrac{|d||r||b|}{d} = \pm br$.

Analogamente, $m' = \dfrac{|a||b|}{d} = \dfrac{|a||dt|}{d} = \dfrac{|a||d||t|}{d} = \pm at$. Temos assim que m' é múltiplo comum de a e b.

Agora, tomando um múltiplo comum c de a e b, com $c \in \mathbb{N}$, temos que existem $u,v \in \mathbb{Z}$ tais que $c = au$ e $c = bv$. Considerando o máximo divisor comum d de a e b, temos que pelo Teorema 5 existem $x_1, y_1 \in \mathbb{Z}$ com $ax_1 + by_1 = d$.

Assim, para verificar que $m'|c$ vamos efetuar a divisão de c por m' afim de se obter um número inteiro.

De $m' = \dfrac{|ab|}{d}$, temos que $m'd = |ab|$. Logo,

$$\frac{c}{m'} = \frac{c \cdot d}{m' \cdot d} = \frac{cd}{|ab|} = \frac{c}{|ab|} \cdot (ax_1 + by_1) = \frac{c.ax_1}{|a||b|} + \frac{c.by_1}{|a||b|} = \pm\frac{c}{b}x_1 \pm \frac{c}{a}y_1.$$

Como $au = c = bv$, tem-se $\dfrac{c}{a} = u$ e $\dfrac{c}{b} = v$ temos que $\dfrac{c}{m'} = \pm vx_1 \pm uy_1 \in \mathbb{Z}$.

Dessa forma, temos que $m'|c$. Assim $m' = \text{mmc}(a,b) = m$. □

Exemplo 13. Já vimos que mdc$(\pm 7519, \pm 8249)$=73.
Logo, mmc$(\pm 7519, \pm 8249)\cdot$mdc$(\pm 7519, \pm 8249) = |(\pm 7519).(\pm 8249)|$.

Portanto, mmc$(\pm 7519, \pm 8249) = \dfrac{7519.8249}{73} = 849647$.

3.5 Equações Diofantinas

Uma relação em n incógnitas $x_1, x_2, x_3, ..., x_n$ da forma

$$f(x_1, x_2, x_3, ..., x_n) = 0$$

é chamada uma equação Diofantina de grau n, quando o interesse é dirigido às suas soluções inteiras $x_1, x_2, x_3, ..., x_n \in \mathbb{Z}$.

A seguir, como exemplo, temos a equação da hiper-esfera de raio 10 no espaço n dimensional

$$x_1^2 + x_2^2 + ... + x_n^2 = 100$$

que pode ser considerada uma equação Diofantina quando as n-uplas de coordenadas inteiras $x_1, x_2, ..., x_n$ são procuradas.

Uma equação Diofantina é linear se ela tiver a forma

$$a_1x_1 + a_2x_2 + ... + a_nx_n = c,\ a_1, a_2, ..., a_n \in \mathbb{Z}.$$

Em particular, trataremos agora as equações Diofantinas lineares com duas variáveis. Ou seja, estudaremos equações da forma

$$ax + by = c,\ a, b, c \in \mathbb{Z}.$$

Teorema 8. Sejam $a, b, c \in \mathbb{Z}$, sendo a e b não ambos nulos.

a) A equação Diofantina $ax + by = c$ admite pelo menos uma solução $x, y \in \mathbb{Z}$ se e somente se, $d =$mdc$(a, b)|c$.

b) Supondo $d|c$ e sendo (x_0, y_0) uma solução particular da equação $ax + by = c$, então o conjunto de todas as soluções será dada por

$$x = x_0 + \frac{b}{d}t,\ y = y_0 - \frac{a}{d}t,\ t \in \mathbb{Z}$$

Demonstração. a) Suponhamos que a equação Diofantina tenha uma solução. Digamos que (x, y) seja essa solução. Então $ax + by = c$. Por outro lado se d=mdc(a,b), então $d|a$ e $d|b$, o que implica que $d|ax + by$, isto é, $d|c$.

Suponha agora $d|c$,. Então, $c = d.l$, para algum $l \in \mathbb{Z}$. Pelo Teorema 5 sabemos que existem $x_1, y_1 \in \mathbb{Z}$ tais que $d = ax_1 + by_1$. Multiplicando ambos os lados da igualdade por l, temos $dl = alx_1 + bly_1$. Ou seja, $c = a(lx_1) + b(ly_1)$ e dessa forma, (lx_1, ly_1) é uma solução de $ax + by = c$.

b) Sejam (x_0, y_0) uma solução particular e $t \in \mathbb{Z}$. Provaremos primeiro que qualquer par de números $\left(x = x_0 + \frac{b}{d}t, y = y_0 - \frac{a}{d}t\right)$, também satisfaz a equação: $ax + by = c$. Temos que $a\left(x_0 + \frac{bt}{d}\right) + b\left(y_0 - \frac{at}{d}\right) = ax_0 + \frac{abt}{d} + by_0 - \frac{abt}{d} = ax_0 + by_0 = c$.

Agora, tomando (x, y) uma solução qualquer de $ax + by = c$, temos que $ax_0 + by_0 = c = ax + by$ o que implica que

$$a(x - x_0) = b(y_0 - y).$$

Sabendo que d =mdc(a,b), temos $d|a$ e $d|b$, dessa forma, existem r e s $\in \mathbb{Z}$ tais que $a = r \cdot d$ e $b = s \cdot d$ e, pela Proposição 12, temos que mdc$\left(\frac{a}{d}, \frac{b}{d}\right) = 1 =$ mdc(r,s). Então temos que,

$$r \cdot d(x - x_0) = s \cdot d(y_0 - y)$$

e, como $d \neq 0$, temos que $r(x - x_0) = s(y_0 - y)$.

Supondo $a \neq 0$, concluímos que $r|s(y_0 - y)$ e aí, como mdc(r,s)=1, temos $r|y_0 - y$. Dessa forma, existe $t \in \mathbb{Z}$, tal que $y_0 - y = rt$. Então $y = y_0 - rt = y_0 - \frac{a}{d}t$.

Segue então que, $r(x - x_0) = s(y_0 - y) = srt$. Como $r \neq 0$, temos $(x - x_0) = st$ e então, $x = x_0 + st = x_0 + \frac{b}{d}t$.

De forma análoga encontramos as mesmas soluções para o caso $b \neq 0$.

Portanto, $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$, com $t \in \mathbb{Z}$ é a solução geral de $ax + by = c$.

□

Exemplo 14. Encontremos a solução geral de $54x + 21y = 906$

Utilizando o algoritmo de Euclides, com $a = 54$ e $b = 21$, determinamos o mdc

$$\begin{aligned} 54 &= 21 \cdot 2 + 12 \\ 21 &= 12 \cdot 1 + 9 \\ 12 &= 9 \cdot 1 + 3 \\ 9 &= 3 \cdot 3 + 0. \end{aligned}$$

Com o último resto zero, temos que o mdc$(54,21) = 3$ e $3|906$, o que implica que a equação tem solução.

Além disso, temos que

$$\begin{aligned} 3 &= 12 - 9 \cdot 1 \\ 3 &= 12 - (21 - 12 \cdot 1) \\ 3 &= (54 - 21 \cdot 2) \cdot 2 - 21 \\ 3 &= 54 \cdot 2 + 21 \cdot (-5). \end{aligned}$$

Multiplicando ambos os lados por 302, temos $906 = 54 \cdot (604) + 21 \cdot (-1510)$. Dessa forma, a solução particular será $(604, -1510)$ e a solução geral

$$x = 604 + 7t,\ y = -1510 - 18t,\ t \in \mathbb{Z}$$

Exemplo 15. Um teatro vende ingressos e cobra $R\$18,00$ por adulto e $R\$7,50$ por criança. Numa noite arrecada-se $R\$900,00$. Quantos adultos e crianças assistiram ao espetáculo, sabendo que eram mais adultos que crianças?

Seja x o número de crianças e y o número de adultos que assistiram ao espetáculo. Dessa forma

$$7,5x + 18y = 900 \text{ com } y > x \geqslant 0$$

Multiplicando-se ambos os membros por dois, temos

$$15x + 36y = 1800$$

Utilizando o algoritmo Euclidiano, com a=15 e b=36, determinamos o mdc(15,36)

$$\begin{aligned} 15 &= 36 \cdot 0 + 15 \\ 36 &= 15 \cdot 2 + 6 \\ 15 &= 6 \cdot 2 + 3 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

Com o último resto zero, temos o $\text{mdc}(15,36) = 3$ e $3|1800$, o que implica que a equação tem solução.

Além disso, temos que

$$\begin{aligned} 3 &= 15 - 6 \cdot 2 \\ 3 &= 15 - (36 - 15 \cdot 2) \cdot 2 \\ 3 &= 15 \cdot 5 + 36 \cdot (-2). \end{aligned}$$

Multiplicando ambos os membros por 600, temos $1800 = 15 \cdot (3000) + 36 \cdot (-1200)$. Dessa forma, uma solução particular será $(3000, -1200)$ e a equação geral sera dada por

$$x = 3000 + 18t,\ y = -1200 - 5t, t \in \mathbb{Z}.$$

Finalmente, como $y > x \geqslant 0$, temos $-1200 - 5t > 3000 + 18t \geqslant 0$. Disso obtemos $t < -247,05$ e $t \geqslant -250$ e portanto, $t \in \{-250, -249, -248\}$

As três possíveis soluções são: $x = 0$ e $y = 50$; $x = 12$ e $y = 45$; e $x = 24$ e $y = 40$.

CAPÍTULO

4

NÚMEROS PRIMOS E SUA DISTRIBUIÇÃO

Neste capítulo, apresentamos alguns dos principais resultados sobre os números primos tais como o teorema fundamental da aritmética, o teorema de decomposição primária e a quantidade de divisores de um número, a partir dos números primos.

Definição 10. Um número $p \in \mathbb{N}$ é denominado primo, se $p > 1$ e seus únicos divisores positivos são p e 1. Denotamos por $\mathbb{P} = \{p \in \mathbb{N} | p \text{ é primo}\}$ o conjunto de todos os números primos. Podemos dizer então que $p \in \mathbb{P} \Leftrightarrow \forall a, b \in \mathbb{N} : p = a.b \Rightarrow a = p$ e $b = 1$ ou $a = 1, b = p$.

Definição 11. Um número natura $n > 1$ é dito composto se ele não é primo. Note que, $n > 1$ é composto se existem $r, s \in \mathbb{N}$ tais que $1 < s \leqslant r < n$ com $n = rs$.

Os primeiros números primos são 2,3,5,7,11,13,17,... entretanto, 4, 6, 8, 9,10,12,14,15,... são os primeiros números compostos.

O Lema de Euclides apresentado no Teorema 6 dá a seguinte propriedade fundamental dos números primos:

Proposição 17. Seja $p \in \mathbb{P}$. Então, para todos $a, b \in \mathbb{N}$ se $p|a \cdot b$ então $p|a$ ou $p|b$.

Demonstração. Suponhamos $p|ab$ e $p \nmid a$.

Se d = mdc(a, p), então, pela Proposição 12, mdc$\left(\frac{a}{d}, \frac{p}{d}\right) = 1$, o que implica que $d|p$ e como p é primo, $d = p$ ou $d = 1$. Mas se $d = p$ então $p|a$, o que contradiz a suposição. Portanto $d =$mdc$(a, p) = 1$ e dessa forma, pelo Teorema 6, temos $p|b$.

Supondo que $p|ab$ e $p \nmid b$ a demonstração é análoga. □

Observação 10. Note que a recíproca da propriedade na Proposição 17 é válida para que um $n \in \mathbb{N}$ seja primo.

Ou seja, dado $n \in \mathbb{N}$, se para todos $a, b \in \mathbb{N}$, $n|ab \Rightarrow n|a$ ou $n|b$, então n é primo. De fato, supondo n composto, temos $n = r \cdot s$ com $1 < s \leqslant r < n$, e assim temos que $n \nmid r$ e $n \nmid s$. Mas $n|rs$ pois $r \cdot s = 1 \cdot n$, contradizendo assim a propriedade na nossa hipótese.

Segundo a Proposição 17 se $5|ab$ então temos certeza que um dos fatores a ou b (ou ambos) é múltiplo de 5. Por outro lado $6|12 = 3 \cdot 4$, porém tanto $6 \nmid 3$ quanto $6 \nmid 4$.

Teorema 9. (Teorema Fundamental da Aritmética)

a) Todo número natural maior do que 1 ou é primo ou é produto de números primos, ou seja, existem $p_1, p_2, ..., p_r \in \mathbb{P}$ tais que

$$n = p_1.p_2 \cdot ... \cdot p_r.$$

b) Se $p_1 \cdot p_2 \cdot ... \cdot p_{r-1} \cdot p_r = q_1 \cdot q_2 \cdot ... \cdot q_{s-1} \cdot q_s$ com $p_1, p_2, ..., p_{r-1}, p_r, q_1, q_2, ..., q_{s-1}, q_s \in \mathbb{P}$ e se $p_1 \geqslant p_2 \geqslant ... \geqslant p_r$ e $q_1 \geqslant q_2 \geqslant ... \geqslant q_s$, então

$$r = s \text{ e } p_1 = q_1; p_2 = q_2; p_3 = q_3, ..., p_r = q_r.$$

Demonstração. a) Se $n = p$ é um número primo, temos $n = p_1$ e dessa forma concluímos a demonstração com $r = 1$. Se n é composto, vamos supor que o resultado seja válido para todo $m \in \mathbb{N}$ com $1 < m < n$, ou seja, podemos supor que existem $p_2, p_3, ..., p_r \in \mathbb{P}$ tais que $m = p_2 \cdot p_3 \cdot ... \cdot p_r$. Seja $\mathbb{S} = \{t \in \mathbb{N} | t > 1 \text{ e } t|n\}$, o conjunto de todos os divisores naturais de n maiores que 1. Sabemos que $\mathbb{S} \neq \emptyset$, pois como $n > 1$ e $n|n$, temos que $n \in \mathbb{S}$. Logo, pelo princípio da indução, existe $p_1 \in \mathbb{S}$ tal que p_1 é mínimo.

Afirmamos que p_1 é primo.

De fato, e p_1 não é primo então, p_1 é composto e dessa forma, existem s e $r \in \mathbb{N}$ com $1 < r \leqslant s < p_1$ tais que $p_1 = r.s$. Assim $r|p_1$ o que implica em $r|n$ e assim $r \in S$, com $r < p_1$. Encontramos aí uma contradição, já que por hipótese p_1 é mínimo em $\mathbb{S}$. Portanto p_1 é primo.

Assim, existe $m \in \mathbb{N}$, tal que $n = p_1.m$. Como $p_1 > 1$ então $m < n$. Podemos escrever então $n = p_1.p_2 \cdot \cdot \cdot \cdot \cdot p_r$

b) Suponhamos que $p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_r = q_1 \cdot q_2 \cdot q_3 \cdot ... \cdot q_s$ com $p_1, p_2, p_3, .., p_r, q_1, q_2, q_3, ..., q_s$ pertencentes $\mathbb{P}$ e $p_1 \leqslant p_2 \leqslant ... \leqslant p_r$ e $q_1 \leqslant q_2 \leqslant ... \leqslant q_s$.

Temos $p_1|q_1 \cdot q_2 \cdot \cdot \cdot \cdot \cdot q_s$ de onde concluímos, aplicando-se repetidas vezes a Proposição 17 que p_1 divide algum dos fatores $q_1, q_2, ..., q_s$. De fato, se $p_1|q_1 \cdot q_2 \cdot q_3 \cdot \cdot \cdot \cdot \cdot q_s$ então $p_1|q_1$ ou $p_1|q_2 \cdot q_3 \cdot \cdot \cdot \cdot \cdot q_s$. Se $p_1|q_2 \cdot q_3 \cdot \cdot \cdot \cdot \cdot q_s$ então $p_1|q_2$ ou $p_1|q_3 \cdot \cdot \cdot \cdot \cdot q_s$. E assim, sucessivamente, até que $p_1|q_{s-1}$ ou $p_1|q_s$.

Dessa forma existe k, $1 \leqslant k \leqslant s$, tal que $p_1|q_k$. Como p_1 e q_k são primos, temos $p_1 = q_k$ e pela hipótese apresentada acima $q_k \geqslant q_1$ e portanto $p_1 \geqslant q_1$.

Da mesma forma, $q_1|p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_r$ e novamente aplicando-se repetida vezes a Proposição 17, temos que q_1 divide algum dos fatores $p_1, p_2, p_3, ..., p_r$. Assim, existe l, em que $1 \leqslant l \leqslant r$, tal que $q_1|p_l$ e portanto $q_1 = p_l$ e como $p_l \geqslant p_1$, temos $q_1 \geqslant p_1$.

Concluímos assim, que $p_1 = q_1$. E , de $p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_r = q_1 \cdot q_2 \cdot q_3 \cdot \cdots \cdot q_s$, temos que $p_2 \cdot p_3 \cdot \cdots \cdot p_r = q_2 \cdot q_3 \cdot \cdots \cdot q_s$.

Continuando este processo concluímos que $p_2 = q_2$, $p_3 = q_3$,...,$p_r = q_i$ com $i \leq s$. Como p_r é primo, garantimos que $i = s$, pois caso contrário teríamos $p_r = q_i \cdot ... \cdot q_s$ o que é absurdo.

Concluímos assim a demonstração. □

Em geral agrupando os fatores primos repetidos, se necessário, e ordenando os primos em ordem crescente, o Teorema Fundamental da Aritmética é formulado como no Teorema a seguir.

Teorema 10. (O teorema da decomposição primária) Para todo número $n \in \mathbb{N}$, tal que $n > 1$, existem únicos primos distintos $p_1, p_2, ..., p_r$, $p_1 < p_2 < ... < p_r$ e únicos $a_1, a_2, a_3, ..., a_r \in \mathbb{N}$ tais que

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_r^{a_r} = \prod_{k=1}^{r} p_k^{a_k}.$$

O produto $\prod_{k=1}^{r} p_k^{a_k}$ chama-se decomposição primária de n.

4.1 A quantidade dos divisores de um número

Como o conjunto dos divisores de um número $n \in \mathbb{N}$ é finito, podemos fazer a referência à sua cardinalidade, isto é, à quantidade dos divisores de n.

Dado $n \in \mathbb{N}$, vamos indicar por

$$\mathscr{T}(n) = |\{t \in \mathbb{N} | t \text{ divide n}\}|$$

a quantidade de divisores naturais de n.

Por exemplo, $\mathscr{T}(n) = 1 \Leftrightarrow n = 1, \mathscr{T}(n) = 2 \Leftrightarrow n = p$ é primo.

Notando que $t|n \Leftrightarrow t \cdot s = n \Leftrightarrow \frac{n}{t} = s$, com $s \in \mathbb{N}$, temos que, $t \cdot \frac{n}{t} = n$ e portanto $\frac{n}{t}|n$ e ainda $t = \frac{n}{\frac{n}{t}}$. Logo,

$$\{t | t \text{ divide n}\} = \left\{\frac{n}{t} | t \text{ divide n}\right\}.$$

Por exemplo, para os divisores de 12, temos que $\{1,2,3,4,6,12\} = \left\{\frac{12}{1}, \frac{12}{2}, \frac{12}{3}, \frac{12}{4}, \frac{12}{6}, \frac{12}{12}\right\}$.

Proposição 18. Para todo $n \in \mathbb{N}$ temos $\prod_{t|n} t = n^{\frac{\mathscr{T}(n)}{2}} = \sqrt{n^{\mathscr{T}(n)}}$.

Ou seja, o produto formado por todos os divisores positivos de n é a potência $\frac{\mathscr{T}(n)}{2}$-ésima de n.

Demonstração. $(\prod_{t|n} t)^2 = \prod_{t|n} t \cdot \prod_{t|n} t = \prod_{t|n} t \cdot \prod_{t|n} \frac{n}{t} = \prod_{t|n} t\frac{n}{t} = \prod_{t|n} n = n^{\mathscr{T}(n)}$.

Agora, extraindo a raiz de ambos os lados da igualdade, temos que $\prod_{t|n} t = \sqrt{n^{\mathscr{T}(n)}}$. □

Podemos determinar $\mathscr{T}(n)$ também a partir da decomposição primária de n.

Proposição 19. Seja $n > 1, n \in \mathbb{N}$ escrito na decomposição primária

$$n = \prod_{k=1}^{r} p_k^{a_k}$$

com $p_1, ..., p_r$ primos distintos e sendo $r, a_1, ..., a_r \in \mathbb{N}$. Um número $t \in \mathbb{N}$ é divisor de n e se, e somente se,

$$t = \prod_{k=1}^{r} p_k^{l_k} \text{ com } 0 \leq l_1 \leq a_1, ..., 0 \leq l_r \leq a_r.$$

Demonstração. Suponha que $t = \prod_{k=1}^{r} p_k^{l_k}$, com $0 \leqslant l_1 \leqslant a_1, ..., 0 \leqslant l_n \leqslant a_r$. Para concluir que t é divisor de n, devemos encontrar $m \in \mathbb{Z}$ tal que $n = t \cdot m$.

Sendo $m = \prod_{k=1}^{r} p_k^{a_k - l_k}$, temos $t \cdot \prod_{k=1}^{r} p_k^{a_k - l_k} = \prod_{k=1}^{r} p_k^{l_k} \cdot \prod_{k=1}^{r} p_k^{a_k - l_k} = \prod_{k=1}^{r} p_k^{a_k} = n$. Como $a_k - l_k \geq 0, \prod_{k=1}^{r} p_k^{a_k - l_k} \in \mathbb{N}$ e dessa forma, t é divisor de n.

Por outro lado se t é divisor de n, temos que $n = k \cdot t$ com $1 < k \leqslant n$. Logo usando a decomposição primária de n e de k temos que $\prod_{k=1}^{r} p_k^{a_k} = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdot \cdots \cdot p_r^{b_r} \cdot t$, com $k = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdot \cdots \cdot p_r^{b_r}$. Então

$$t = p_1^{a_1 - b_1} \cdot p_2^{a_2 - b_2} \cdot p_3^{a_3 - b_3} \cdot \cdots \cdot p_r^{a_r - b_r} = p_1^{l_1} \cdot p_2^{l_2} \cdot p_3^{l_3} \cdot \cdots \cdot p_r^{l_r}.$$

Portanto $t = \prod_{k=1}^{r} p_k^{l_k}$ com $0 \leqslant l_i \leqslant a_i$, $i = 1, ...r$, fazendo com que a afirmação seja verdadeira. □

Corolário 2. Seja $n \in \mathbb{N}$ escrito como $n = \prod_{k=1}^{r} p_k^{a_k}$, com $p_1, p_2, ..., p_r$ primos distintos e $a_1, a_2, ..., a_r \in \mathbb{N}$. Então, $\mathscr{T}(n) = \prod_{k=1}^{r} (a_k + 1)$

Demonstração. Pela Proposição 10 temos que os divisores $t \in \mathbb{N}$ de n correspondem biunivocamente às r-uplas $(l_1, l_2, ..., l_r)$ com $0 \leqslant l_1 \leqslant a_1, ..., 0 \leqslant l_r \leqslant a_r$. Portanto, $\mathscr{T}(n)$ é a quantidade dessas r-uplas. Mas na k-ésima coordenada temos as $a_k + 1$ possibilidades $0, 1, 2, ..., a_k$ para escolhermos $l_k (1 \leqslant k \leqslant r)$.

Isso nos fornece um total de $(a_1 + 1).(a_2 + 1)....(a_k + 1)$ escolhas e verifica a afirmação. □

Corolário 3. Seja $n \in \mathbb{N}$. Então n é um quadrado perfeito $\Leftrightarrow$ $\mathscr{T}(n)$ é ímpar.

Demonstração. Seja $n = \prod_{k=1}^{r} p_k^{a_k}$ a decomposição primária de n. Temos que n é um quadrado perfeito se, e somente se, todos os expoentes $a_1, a_2, ..., a_r$ são pares. Temos ainda que $a_1, a_2, ..., a_r$ são pares se, e somente se, $a_1+1, a_2+1, ..., a_r+1$ são ímpares, com o produto $(a_1+1)\cdot(a_2+1)\cdot\cdots\cdot(a_r+1)$ ímpar pois o produto ímpar é obtido quando os fatores são ímpares.Portanto $\mathscr{T}(n)$ é ímpar. □

A decomposição primária é muito útil para determinar o mdc e o mmc de dois números.

Dados dois números $n, m \in \mathbb{N}$, e considerando os primos distintos $p_1, ..., p_r$ que dividem n ou m, existem expoentes não-negativos $a_1, ..., a_r, b_1, ..., b_r \in \mathbb{N}_0$ tais que, simultaneamente,

$$n = \prod_{k=1}^{r} p_k^{a_k} \text{ e } m = \prod_{k=1}^{r} p_k^{b_k}. \tag{4.1}$$

Proposição 20. Sejam $n, m \in \mathbb{N}$ escritos na forma 4.1. Então,

$$\text{mdc}(m,n) = \prod_{k=1}^{r} p_k^{\min(a_k,b_k)} \text{ e } \text{mmc}(m,n) = \prod_{k=1}^{r} p_k^{max(a_k,b_k)}.$$

Demonstração. Mostremos inicialmente que mdc(m,n)= $\prod_{k=1}^{r} p_k^{\min(a_k,b_k)}$.

Como $\min(a_k,b_k) \leq a_k$ e $\min(a_k,b_k) \leq b_k$, temos, pela Proposição 19, que o produto $\prod_{k=1}^{r} p_k^{\min(a_k,b_k)}$ certamente é divisor comum de m e n. Por outro lado, sendo t um número da forma $t = \prod_{k=1}^{r} p_k^{l_k}$, em que t é um divisor comum de m e n, devemos ter $0 \leqslant l_k \leqslant a_k$ e $0 \leqslant l_k \leqslant b_k$, o que implica que $0 \leqslant l_k \leqslant \min(a_k,b_k)$. Logo $t | \prod_{k=1}^{r} p_k^{\min(a_k,b_k)}$ e portanto $\prod_{k=1}^{r} p_k^{\min(a_k,b_k)}$ e o máximo divisor comum entre m e n. Ou seja, mdc(m,n)= $\prod_{k=1}^{r} p_k^{\min(a_k,b_k)}$.

Agora, mostremos que $\text{mmc}(m,n) = \prod_{k=1}^{r} p_k^{max(a_k,b_k)}$.

Seja $t = \prod_{k=1}^{r} p_k^{l_k} \cdot s$ $(s \in \mathbb{N})$ um múltiplo comum de m e n, sendo $l_k \geqslant a_k$ e também $l_k \geqslant b_k$ e portanto, $l_k \geqslant \max(a_k,b_k)$. Como $\max(a_k,b_k)$ é o menor dos possíveis expoentes de l_k e $\prod_{k=1}^{r} p_k^{max(a_k,b_k)} | \prod_{k=1}^{r} p_k^{l_k}$ então $\prod_{k=1}^{r} p_k^{max(a_k,b_k)} | t$. Além disso, $\prod_{k=1}^{r} p_k^{max(a_k,b_k)}$ é, múltiplo de m e n. Portanto, $\prod_{k=1}^{r} p_k^{max(a_k,b_k)}$ é um múltiplo de m e n. Portanto, $\prod_{k=1}^{r} p_k^{max(a_k,b_k)}$ é o mmc(m,n). □

4.2 A decomposição primária de n!

A seguir estudaremos qual é a decomposição primária do número n! para qualquer $n \in \mathbb{N}$.

Sendo p um número primo e $p|n!$, temos que $p|1\cdot 2\cdot 3\cdot \ldots \cdot n$ e daí, uma aplicação repetida da Proposição 17 mostra que p tem que dividir um dos fatores $2, 3, ..., n$ deste produto.

Em particular, $n!$ não pode ser divisível por nenhum primo maior que n. Por outro lado, qualquer primo p com $p \leqslant n$ aparece no desenvolvimento de $n!$ e já podemos afirmar que a decomposição primária de $n!$ é da forma

$$n! = \prod_{k=1}^{r} p_k^{a_k}$$

em que $p_1 = 2, p_2 = 3, p_3 = 5, ..., p_r \leqslant n < p_{r+1}$, ou seja, $p_1, p_2, p_3, ..., p_r$ são todos os primos menores ou iguais a n e os expoentes $a_1, a_2, ..., a_r$ são números naturais os quais devemos determinar.

Para representar essa decomposição primária usaremos uma nova notação, a saber

$$n! = \prod_{p \in \mathbb{P}} p^{a_p(n)}$$

Aqui p é considerado seu próprio índice e o índice dos expoentes $a_p(n) \in \mathbb{N}_0$, sendo que p varia sobre $\mathbb{P}$ com a condição $a_p(n) = 0$ se $p > n$. Diante disso, a questão é, quais são os expoentes a_p(n) quando $p \leqslant n$?

Exemplo 16. Encontremos $a_p(40)$.

Para simplificar a notação escrevemos a_p no lugar de $a_p(40)$. Então

$$40! = 2^{a_2} \cdot 3^{a_3} \cdot 5^{a_5} \cdot 7^{a_7} \cdot 11^{a_{11}} \cdot 13^{a_{13}} \cdot 17^{a_{17}} \cdot 19^{a_{19}} \cdot 23^{a_{23}} \cdot 29^{a_{29}} \cdot 31^{a_{31}} \cdot 37^{a_{37}}.$$

O objetivo agora é determinar os expoentes $a_2, a_3, ..., a_{37}$. De imediato sabemos que $a_{37} = a_{31} = a_{29} = a_{23} = 1$.

Agora, 19 divide 19 e 38. Logo $a_{19} = 2$, ocorrendo o mesmo com a_{17}.

Temos $a_{13} = 3$, pois 13 divide 13,26,39. Da mesma forma, $a_{11} = 3$ e $a_7 = 5$.

Perceba ainda que temos 8 fatores 5 em 40!, já que 5 divide 5, 10 ,15, 20, 25, 30, 35, 40, porém no fator 25 temos mais um fator 5 ainda não contado, já que, $25 = 5^2$. Portanto $a_5 = 9$.

O número 3, aparece 13 vezes nos divisores 3,6,9,...,39, mais 4 vezes nos divisores 9,18,27,36 e mais uma terceira vez em 27. Isso dá um total de 18 fatores 3 em 40!. Portanto $a_3 = 18$.

Finalmente contamos $a_2 = 38$, dividindo a 20 fatores em 2,4,6,8,...,40, mais 10 fatores em 4,8,12,...,40, mais 5 fatores em 8,16,24,32,40, mais 2 fatores em 16,32 e mais um fator 2 em 32.

Logo teremos $40! = 2^{38} \cdot 3^{18} \cdot 5^9 \cdot 11^3 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23 \cdot 29 \cdot 31 \cdot 37$.

Para o caso geral consideramos a seguinte definição.

Definição 12. Para cada número real x indicamos por $[x]$ como sendo o maior inteiro contido em$x$ ou ainda, a parte inteira do número x. Escreveremos x=[x]+r, em que $[x] \in \mathbb{Z}$ e $r \in \mathbb{R}$, com $0 \leqslant r < 1$.

Por exemplo, usando a definição anterior temos que $\left[\frac{17}{4}\right] = \left[\frac{19}{4}\right] = 4$; $[\sqrt{5}] = 2$; $[\pi] = 3$; $[-\pi] = -4$.

Teorema 11. Para cada $n \in \mathbb{N}$ a decomposição primária de n! é dada por

$$n! = \prod_{p \in \mathbb{P}} p^{a_p(n)}$$

onde os expoentes $a_p(n)$ são calculados por

$$a_p(n) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right].$$

Antes de provarmos o Teorema 11 acima observamos que a soma $\sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right]$ que é formalmente uma soma infinita na verdade contém finitas parcelas não-nulas, já que $\left[\frac{n}{p^k} \right] = 0$ sempre quando $p^k > n$. Particularmente $a_p(n) = 0$, se $p > n$. Isto significa que no produto para n!, que é formalmente infinito, na verdade aparecem automaticamente só os primos $p \leqslant n$.

Demonstração. Seja p um número primo qualquer menor ou igual a n.

Existe um único $l_1 \in \mathbb{N}_0$ tal que

$$l_1 p \leqslant n < (l_1 + 1)p. \tag{4.2}$$

Da mesma forma, existe um único $l_2 \in \mathbb{N}_0$ tal que $l_2 p^2 \leq n < (l_2 + 1)p^2$.

Em geral, para todo $k \in \mathbb{N}$ existe um único $l_k \in \mathbb{N}_0$ tal que $l_k p_k \leq n < (l_k + 1)p^k$.

Agora, vamos fazer a contagem da quantidade de fatores p em n!.

De 4.2 temos $l_1 \leqslant \frac{n}{p} < l_1 + 1$ e, portanto, há l_1 fatores p em n!. Esses fatores são $p, 2p, 3p, ..., l_1 p$.

Analogamente temos $l_2 \leqslant \frac{n}{p^2} < l_2 + 1$ e, portanto, há l_2 fatores p em n! que ainda não haviam sido contados. E são eles $p^2, 2p^2, ..., l_2 p^2$.

Em geral, temos $l_k \leqslant \frac{n}{p^k} < l_k + 1$ e, portanto, l_k fatores p em $n!$ que ainda não haviam sido contados. E são eles $p^k, 2p^k, ..., l_k p^k$.

Portanto, no total, a quantidade de fatores p em que $n!$ será dada por

$$a_p(n) = l_1 + l_2 + l_3 + \cdots + l_k + \cdots$$

Mas de $l_k \leq \frac{n}{p^k} < l_k + 1$, segue que $l_k = \left[\frac{n}{p^k} \right]$ e, portanto, $a_p(n) = \sum_{k=1}^{\infty} \left[\frac{n}{p_k} \right]$. □

Uma importante observação é que $a_2(n) \geqslant a_3(n) \geqslant a_5(n) \geqslant ... \geqslant a_p(n) \geqslant a_q(n) \geqslant ...$ se $p < q$. Logo, uma consequência disso é, por exemplo, que $n!$ termina em $a_5(n)$ zeros.

Exemplo 17. O número 357! termina em quantos zeros?

Para essa pergunta devemos determinar o expoente do primo 5 na decomposição primária de 357!.

Assim, $a_5(357) = \sum_{k=1}^{\infty} \left[\frac{357}{5^k}\right] = \left[\frac{357}{5}\right] + \left[\frac{357}{5^2}\right] + \left[\frac{357}{5^3}\right] = 71 + 14 + 2 = 87.$

E portanto, pela observação apresentada acima, 357! termina em 87 zeros.

Exemplo 18. Considerando o número 2000! qual é a maior potência de 165 que o divide?

Vamos primeiro encontrar a decomposição primária de 165, $165 = 3 \cdot 5 \cdot 11$ e para encontrar a maior potência de 165 que divide 2000! vamos determinar o expoente de 11 na decomposição primária de 2000! Então

$$a_{11}(2000) = \sum_{k=1}^{\infty} \left[\frac{2000}{11^k}\right] = \left[\frac{2000}{11}\right] + \left[\frac{2000}{11^2}\right] + \left[\frac{2000}{11^3}\right] = 181 + 16 + 1 = 198$$

Logo é a 198-ésima a maior potência de 165 que divide 2000!

4.3 Estimativas sobre quantidade de primos

Teorema 12. (Teorema de Euclides) O conjunto $\mathbb{P}$ dos números primos é infinito.

Demonstração. Vamos supor que o conjunto dos números primos seja finito, ou seja, que $\mathbb{P} = \{p_1, p_2, p_3, ..., p_r\}$.

Vamos agora, considerar um número natural $n = p_1 \cdot p_2 \cdot \cdots \cdot p_r + 1$. Pelo Teorema Fundamental da Aritmética, este número n $(n > 1)$ é divisível por algum primo q. Como estamos supondo que o conjunto dos números primos é finito, então $q = p_k$ para algum $k \in \{1, 2, 3, ..., r\}$. Então, $q|n \Rightarrow q|p_1 \cdot p_2 \cdot \cdots \cdot p_k \cdot \cdots \cdot p_r + 1$. Como $q = p_k$ e $q|p_1 \cdot p_2 \cdot \cdots \cdot p_k \cdot \cdots \cdot p_r$, então $q|1$, o que é um absurdo, já que q é primo. Logo, nenhum conjunto finito pode abranger todos os primos. □

Proposição 21. Para o n-ésimo número primo p_n temos que $p_n \leqslant 2^{2^{n-1}}$.

Demonstração. Faremos a demonstração pelo Princípio da Indução Finita.

Para $n = 1$ facilmente verificamos a veracidade da proposição, pois

$$p_1 = 2^1 \leqslant 2^{2^{1-1}}.$$

Agora, vamos supor a veracidade da proposição para os n primeiros primos e demonstraremos a veracidade para o $(n+1)$-ésimo primo. Ou seja, suponhamos que

$$p_1 \leqslant 2^{2^0}$$

$$p_2 \leqslant 2^{2^1}$$

$$p_3 \leqslant 2^{2^2}$$
$$\vdots$$
$$p_n \leqslant 2^{2^{n-1}}$$

Tomaremos um primo q tal que $q|p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n + 1$. Então sabemos que $q > p_n$, o que equivale a dizer que $q \geqslant p_{n+1}$.

Por outro lado, $q \leqslant p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n + 1$ e então,

$$p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n \leqslant 2^{2^0} \cdot 2^{2^1} \cdot 2^{2^2} \cdot \cdots \cdot 2^{2^{n-1}} \leqslant 2^{2^{1+2+4+\cdots+2^{n-1}}}.$$

Calculando a soma $1+2+4+...+2^{n-1}$, que é a soma dos n termos de uma progressão geométrica de razão 2 e primeiro termo 1 temos que

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

Então,

$$p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n \leqslant 2^{2^n-1}.$$

Logo,

$$p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_n + 1 \leqslant 2^{2^n-1} + 1.$$

E então, de $p_{n+1} \leq q \leq p_1.p_2 \cdot \cdots \cdot p_n + 1$, temos que

$$p_{n+1} \leqslant 2^{2^n-1} + 1 \leqslant 2^{2^n-1} + 2^{2^n-1} = 2^{2^n} = 2^{2^{(n+1)-1}}.$$

Assim, verificamos a veracidade da proposição. □

Uma melhor estimativa para o n-ésimo primo p_n será dada na próxima proposição. Para provar este resultado usaremos o Teorema de Tchebychef apresentado a seguir, sem demonstração.

Teorema 13. (Teorema de Tchebychef) Se $m \in \mathbb{N}$, $m \geqslant 2$, existe um primo p com $m < p < 2m$.

Proposição 22. Para o n-ésimo número primo p_n temos que $p_n \leqslant 2^n$.

Demonstração. Faremos a demonstração pelo Princípio da Indução Finita.

Para $n = 1$, como o primeiro número primo é $p_1 = 2$, temos claramente que $2 = p_1 \leqslant 2^1$.

Agora, suponhamos a veracidade para o n-ésimo número primo e mostremos para o n+1-ésimo.

Do Teorema 13 temos que $\forall n = 1, 2, 3, ...$ tomando $m = p_n$ deveremos ter $p = p_{n+1}$ e tem-se $p_n < p_{n+1} < 2p_n$. Como por hipótese $p_n \leq 2^n$, temos $p_n < p_{n+1} \leq 2.2^n \Rightarrow p_n < p_{n+1} \leq 2^{n+1}$.

Portanto $p_n \leqslant 2^n$, para todo $n \in \mathbb{N}$. □

Definição 13. Um par de números (p,p+2) é denominado um gêmeo de primos se ambos p e p+2 são primos.

Exemplo 19. Os pares (3,5);(5,7);(11,13);(17,19);(29,31);(41,43);(59,61);(71,73) são os gêmeos de primos com $p \leqslant 97$.

É importante observar que ainda é desconhecido se existe uma quantidade infinita de gêmeos de primos.

Definição 14. Para todo $x \in \mathbb{R}, x \geqslant 0$ define-se a função $\Pi(x)$ por

$$\Pi(x) = |\{p \in \mathbb{P} | p \leqslant x\}|$$

isto é, $\Pi(x)$ é a quantidade dos números primos menores ou iguais a x.

Por exemplo, temos $\Pi(x) = 0$ se $0 \leqslant x < 2; \Pi(x) = 1$ se $2 \leqslant x < 3$; $\Pi(x) = 2$ se $3 \leqslant x < 5$. Em geral se $p_1 = 2, p_2 = 3, p_3 = 5, ..., p_{23} = 97, ...$ é a sequência dos números primos em ordem natural, então

$$\Pi(x) = r \text{ se } p_r \leqslant x < p_{r+1}, \text{ com } r \in \{1, 2, 3, ...\}$$

Uma das grandes descobertas do final do século passado (1876) é o chamado Teorema dos números primos, o qual descreve o comportamento assintótico da função $\Pi(x)$. Esse Teorema leva os nomes dos matemáticos Cauchy, Hadamard e De La Valéi Poussin e será apresentado a seguir sem demonstração.

Teorema 14. Para a função $\Pi(x)$ temos que

$$\lim_{x \to \infty} \frac{\Pi(x)}{\frac{x}{\ln x}} = 1.$$

Ou se x é grande, a quantidade dos números primos menores ou iguais a x é aproximadamente igual a $\frac{x}{\ln x}$.

4.4 Decomposição de números e o crivo do Eratóstenes

Iniciamos esta seção com o seguinte resultado relacionado à decomposição de números naturais.

Proposição 23. a) Sejam $n, r, s \in \mathbb{N}$ tais que $n = r.s$, com $1 \leqslant s \leqslant r \leq n$. Então, $s \leqslant \sqrt{n} \leqslant r$.

b) Se n for composto, então existem $r, s \in \mathbb{N}$ tais que $1 < s \leqslant \sqrt{n} \leqslant r < n$ e $n = rs$.

Demonstração. a) Vamos supor $s \leqslant r < \sqrt{n}$.

Dessa desigualdade temos que $n = r \cdot s < \sqrt{n}\sqrt{n} = n$, ou seja, $n < n$ o que é um absurdo.

Analogamente, supondo que $\sqrt{n} < s \leqslant r$, temos que $n = \sqrt{n}\sqrt{n} < s \cdot r = n$, o que é um absurdo.

b) É uma consequência direta do item (a).

□

Corolário 4. Se $n \in \mathbb{N}$ é composto, então n é divisível por algum primo $p \leqslant \sqrt{n}$.

Demonstração. Seja n um número composto, então pela Proposição 23 (b) existem $r, s \in \mathbb{N}$ tais que $n = r...$ com $1 < s \leqslant \sqrt{n} \leqslant r < n$.

I) Se s é primo, $s|n$ e $s \leqslant \sqrt{n}$.

II) Se s é composto, existe uma fatoração para s, $s = p_1.q$ tal que p_1 seja primo. Logo, temos que $p_1|s$ e $s|n$ o que implica que $p_1|n$. Como $s \leqslant \sqrt{n}$ concluímos que $p_1 \leqslant \sqrt{n}$.

De I) e II), temos que se n é composto, existe um primo $p \leqslant \sqrt{n}$ tal que $p|n$. □

Os resultados acima têm importância prática na procura de números primos e é a base do chamado crivo de Eratóstenes, que introduziremos a seguir.

4.4.1 Crivo de Eratóstenes

Desejamos determinar os primos menores ou iguais a n para um dado $n \in \mathbb{N}$, $n \geqslant 2$. Para isso escrevemos os números

$$2, 3, 4, 5, 6, 7, 8, ..., n.$$

Guardamos o 2 como primo e riscamos todos os números pares $4 \leqslant 2k \leqslant n$. Depois guardamos o 3 e riscamos todos os múltiplos de 3 com $6 \leqslant 3k \leqslant n$.

O próximo número não riscado é o primo 5. Riscamos seus múltiplos $10 \leqslant 5k \leqslant n$ e continuamos desta maneira.

Vemos que, depois de riscar os múltiplos de todos os primos até o maior primo $p \leqslant \sqrt{n}$, sobram somente os números primos até n.

Por exemplo, para $n = 100$. Depois de riscar entre os números $2, 3, 4, 5, 6, ..., 100$ os múltiplos próprios de $2, 3, 5$ e 7, sobram os 25 primos $2, 3, 5, 7, 11, 13, ..., 83, 89, 97$. Isto é claro pelo Corolário 4, pois qualquer $n \leqslant 100$ composto é múltiplo de um dos primos $2, 3, 5, 7 \leqslant 10 = \sqrt{100}$.

Também podemos pensar da seguinte forma. Para se verificar se um dado número n é primo ou composto, só é preciso testar como possíveis divisores os primos $p \leqslant \sqrt{n}$. Se nenhum deles divide, n será primo.

Portanto, para ver se um número $n \leqslant 100$ é primo ou não, os quatro testes $2|n, 3|n, 5|n, 7|n$ são suficientes dos quais $2|n$ e $5|n$ tem resposta óbvia.

Da mesma maneira, somente os testes com (no máximo) os primos $p \leqslant 13$ são suficientes para conseguir uma possível decomposição de um qualquer $n \leqslant 200; p \leqslant 31$ para qualquer $n \leqslant 1000; p \leqslant 97$ para $n \leqslant 10000$.

Proposição 24. Seja $n \in \mathbb{N}$ ímpar. Entre os pares inteiros (x,y) com $0 \leqslant y < x \leqslant n = x^2 - y^2$ e os pares (r,s) com $1 \leqslant s \leqslant r \leqslant n = rs$ existe uma correspondência biunívoca natural.

Demonstração. Se $n = x^2 - y^2$ com $0 \leqslant y < x \leqslant n$, fazendo $r = x + y$ e $s = x - y$ temos que $n = x^2 - y^2 = x^2 - xy + xy - y^2 = (x+y)(x-y) = rs$.

Seja, reciprocamente $n = rs$ com $1 \leqslant s \leqslant r \leqslant n$. Como n é ímpar temos que r e s são ímpares e assim $r+s$ e $r-s$ são pares. Logo, $\frac{r+s}{2}$ e $\frac{r-s}{2}$ são inteiros.

Fazendo $x = \frac{r+s}{2}$ e $y = \frac{r-s}{2}$, temos que $x, y \in \mathbb{N}_0$ e também $0 \leqslant y < x \leqslant n$ com $x^2 - y^2 = \frac{(r+s)^2 - (r-s)^2}{4} = \frac{r^2 + 2rs + s^2 - r^2 + 2rs - s^2}{4} = \frac{4rs}{4} = rs = n.$ □

Da Proposição 24 podemos concluir as seguintes consequências imediatas.

Seja $n \in \mathbb{N}$ ímpar.

a) n possui tantas decomposições como diferença de dois quadrados$n = x^2 - y^2$ quantas decomposições multiplicativas distintas $n = r \cdot s$.

b) n é primo, se e somente se $n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2$ é a única decomposição de n como diferença de dois quadrados. Aqui basta notar que n é primo se, e somente se, $n = n \cdot 1$, fazendo com que $r = n$ e $s = 1$.

Exemplo 20. a) Para $n = 33 = 33 \cdot 1 = 11 \cdot 3$ temos as decomposições correspondentes como diferença de dois quadrados:

I) Para $n = 33 = 33 \cdot 1$, temos que

$$r = 33 \text{ e } s = 1 \text{ e então } x = \frac{33+1}{2} = 17; y = \frac{33-1}{2} = 16.$$

Logo, $33 = 17^2 - 16^2$.

II) Para $n = 33 = 11 \cdot 3$ temos que

$$r = 11 \text{ e } s = 3 \text{ e então } x = \frac{11+3}{2} = 7 \text{ e } y = \frac{11-3}{2} = 4.$$

Logo, $33 = 7^2 - 4^2$.

b) Para $n = 9 = 9 \cdot 1 = 3 \cdot 3$ temos que

$$9 = 5^2 - 4^2 = 3^2 - 0^2.$$

c) Em geral, para $n = pq = pq \cdot 1 = p \cdot q$ onde $p \geqslant q$ são primos, temos as decomposições correspondentes como diferença de dois quadrados:

$$pq = \left(\frac{pq+1}{2}\right)^2 - \left(\frac{pq-1}{2}\right)^2 = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$$

d) Para $n = 105 = 105 \cdot 1 = 35 \cdot 3 = 21 \cdot 5 = 15 \cdot 7$, temos que

$$105 = 63^2 - 62^2 = 19^2 - 16^2 = 13^2 - 8^2 = 11^2 - 4^2.$$

Observação 11. A descoberta de uma decomposição de um número ímpar n como diferença de dois quadrados pode ser favorável quando n é "quase um quadrado perfeito", isto é, quando $n = r \cdot s$ com $y = r - s$ "pequeno". Isso pode servir para descobrir a decomposição primária de tal número.

Vejamos a seguir alguns exemplos.

Exemplo 21. Vejamos se o número $n = 2438323$ é primo ou não. Temos $\sqrt{n} = \sqrt{2438323} = 1561,51...$ e daí, para verificar se esse número é primo, pelo Corolário 4 deveríamos testar a divisibilidade desse número n por algum primo $p \leqslant 1561$. (Pelo Corolário 4). Como isso seria inviável, vamos escrever n na forma de diferença de dois quadrados $n = x^2 - y^2$, ou seja, $y^2 = x^2 - n$. Começaremos com x igual ao menor número inteiro maior que 1561, isto é $x = 1562$ e então $x^2 = 2439844$ e $y^2 = 1521$, o que implica que $y = 39$.

Dessa forma, pela Proposição 24 temos a decomposição

$$n = (1562 + 39) \cdot (1562 - 39) = 1601 \cdot 1523.$$

Logo, n não é primo. Mais ainda, a decomposição acima é a decomposição primaria de n, pois pelo Corolário 4 podemos verificar que 1601 e 1523 são realmente primos, observando que n não foi divisível por nenhum primo $p \leqslant 37$.

Exemplo 22. Para determinar a decomposição de $n = 17473$, calculamos $\sqrt{n} = 132,18...$ e colocando $x = 133, 134, ...$ vemos que na quinta tentativa, para $x = 137$, teremos $137^2 - n = 36^2$. Mais uma vez descobrimos a decomposição $n = (137 + 36)(137 - 36) = 173 \cdot 101$.

Exemplo 23. Seja $n = p(p+2)$ o produto de primos gêmeos sem que se saiba disso previamente. Então, $p < \sqrt{n} = \sqrt{p(p+2)} < \sqrt{p^2 + 2p + 1}\sqrt{(p+1)^2} = p + 1$. Logo no primeiro passo para $x = p + 1$ temos que

$$(p+1)^2 - n = (p+1)^2 - p(p+2) = 1^2.$$

Dessa forma, a decomposição será dada por $n = [(p+1)+1][(p+1)-1]$.

Seguem a seguir mais algumas observações a respeito de números primos.

4.4.2 A conjectura de Goldback

Christian Goldback (1690-1754) estabeleceu a seguinte conjectura que até hoje não pôde ser provada.

Proposição 25. (Conjectura de Goldback) Todo número par $n > 4$ é a soma de dois primos ímpares.

Exemplo 24.

$$6 = 3+3$$

$$8 = 3+5$$

$$10 = 7+3 = 5+5$$

$$12 = 7+5$$

$$\dots$$

$$100 = 97+3 = 89+11 = 83+17 = 71+29 = 59+41 = 53+47.$$

Pelo Teorema 13 de Tchebychef existe sempre um primo entre qualquer número e seu dobro. Por outro lado, existem intervalos de comprimento arbitrário n, livre de números primos, como mostraremos a seguir.

Proposição 26. Para todo $n \in \mathbb{N}$ existe um $k_n \in \mathbb{N}$ tal que os números consecutivos

$$k_n+1, k_n+2, k_n+3, ..., k_n+n$$

são todos compostos.

Demonstração. Dado $n \in \mathbb{N}$, escolhemos $k_n = (n+1)!+1$ em que podemos observar que $2,3,4,...,(n+1)$ todos dividem $(n+1)!$ e daí,

$$2|(n+1)!+2 = k_n+1$$

$$3|(n+1)!+3 = k_n+2$$

$$4|(n+1)!+4 = k_n+3$$

$$\vdots$$

$$n|(n+1)!+n = k_n+(n-1)$$

$$(n+1)|(n+1)!+(n+1) = k_n+n,$$

o que mostra que $k_n+1, k_n+2, ..., k_n+n$ são compostos. □

4.4.3 Progressão aritméticas e primos

Dados $a, b \in \mathbb{N}_0$ com $b > 0$, podemos considerar a progressão aritmética

$$(a+bn)_{n\in\mathbb{N}_0} = (a, a+b, a+2b, a+3b, ...)$$

e nos perguntar sobre os números primos que possivelmente apareçam nela.

Note que para que um dos $a+bn$ com $n \geqslant 1$ possa ser primo é claramente necessário que mdc$(a,b) = 1$, pois mdc(a,b) divide cada $a+bn$.

Exemplo 25. No caso $a = 0, b = 1$, temos que $(0+1n)_{n\in\mathbb{N}_0} = (0,1,2,3,4,...)$, que é a sequência dos números naturais, a qual contém infinitos primos (por Euclides). Além disso, se $a = 1$ e $b = 2$, temos que $(1+2n)_{n\in\mathbb{N}_0} = (1,3,5,...)$, que é a sequência dos números ímpares e esta contém infinitos primos.

Este é mais um resultado clássico e profundo do século passado, devido a Dirichlet(1837) que queremos citar, porém sem demonstração.

Teorema 15. Se $a, b \in \mathbb{N}_0$ são dois números com $b > 0$ e mdc$(a,b) = 1$, então, na progressão aritmética $(a+bn)_{n\in\mathbb{N}}$ aparecem infinitos números primos.

Como mais um caso particular do teorema de Dirichlet apresentamos o seguinte exemplo.

Exemplo 26. Para $b = 4$ e $a = 3$ existem infinitos primos da forma $4n+3, n \in \mathbb{N}$.

Inicialmente observamos que é fácil verificar que dados $k_1, k_2, ..., k_r \in \mathbb{N}$, então o produto $(4k_1+1)(4k_2+1)\cdot ...\cdot(4k_r+1)$ tem a forma $4l+1$ com $l \in \mathbb{N}$. Ou seja, que um produto de números que deixam resto 1 quando divididos por 4 é um número do mesmo tipo.

Agora suponha que $\overline{\mathbb{P}} = \mathbb{P} \cap \{4n+3 | n = 0,1,2,3,...\}$ é finito, digamos

$$\overline{\mathbb{P}} = \{p_1 = 3; p_2 = 7; ...; p_r\}.$$

Considere o número ímpar $N = 4p_1 \cdot p_2 \cdot \cdots \cdot p_r - 1 = 4(p_1 \cdot p_2 \cdot \cdots \cdot -1) + 3 > 1$, e seja $N = q_1 \cdot q_2 \cdot \cdots \cdot q_s$, com $q_1, q_2, ..., q_s$ primos, sabemos que todo número ímpar é da forma $4k+1$ ou $4k+3$. Como N é da forma $4l+3, l \in \mathbb{N}$, temos pela observação acima que nem todos os q_i podem ter a forma $4k_i+1$, ou seja, existe um $q_i \in \overline{\mathbb{P}}$, digamos $q_i = p_j$ para algum $j = 1, ..., r$. Mas então segue que $q_i | 4 \cdot p_1 \cdot p_2 \cdot \cdots \cdot p_j \cdot \cdots \cdot p_r$ e $q_i | N \Rightarrow q_i | 4 \cdot p_1 \cdot p_2 \cdot \cdots \cdot p_j \cdot \cdots \cdot p_r - N$.

Sabemos ainda que como $N = 4p_1p_2 \cdots p_j \cdots p_r - 1$, então $4p_1p_2 \cdots p_j \cdots p_r - N = 1$ e $q_i | 1$ o que é absurdo pois q_i é primo. Portanto, $\overline{\mathbb{P}}$ não é finito, o que nos faz concluir que existe, infinitos primos da forma $4n+3$.

4.4.4 Polinômios e primos

Encerraremos este capítulo, pensando na seguinte pergunta. Será que existe alguma expressão polinomial $f(n) = a_s n^s + a_{s-1} n^{s-1} + ... + a_1 n^1 + a_0$ com coeficientes inteiros, que forneça a sequência dos números primos, ou pleo menos que forneça somente primos?

Vamos analisar o seguinte exemplo que apresenta essa proposta.

Exemplo 27. Para $f(n) = n^2 + n + 41$ temos $f(n) \in \mathbb{P}$ para todo $n = 1, 2, 3, ..., 39$. Entretanto, $f(40) = 40^2 + 40 + 41 = 1681 = 41^2$ e $f(41) = 41^2 + 41 + 41 = 1763 = 41.43$ não são primos.

Veremos a seguir que a resposta geral para a pergunta acima é não. Nenhum polinômio não constante pode assumir somente números primos.

Proposição 27. Seja $f(n) = a_s n^s + a_{s-1} n^{s-1} + ... + a_1 n^1 + a_0$ uma expressão polinomial com coeficientes $a_0, a_1, ..., a_s \in \mathbb{Z}$ e $a_s > 0, s \geqslant 1$. Então a sequência $(f(n))_{n\mathbb{N}}$ assume infinitos valores naturais compostos.

Demonstração. Sabemos que $f(n)$ pode assumir somente finitos valores negativos, uma vez que $a_s > 0, s \geqslant 1$. Além disso, se $f(n)$ sempre é composto, não há nada para provar. Podemos supor então que exista $n_0 \in \mathbb{N}$ tal que $f(n_0) = p$ é primo e $f(n) > 0$ para $n \geqslant n_0$. Para todo $t \in \mathbb{N}$ temos que

$$\begin{aligned} f(n_0 + t \cdot p) \cdots a_s(n_0 + t \cdot p)^s + \cdots + a_s(n_0 + t \cdot p) + a_0 &= a_s n_0^s + ... + a_1 n_0 + a_0 + k_t p \\ &= f(n_0) + k_t p \\ &= p + k_t p \\ &= p(1 + k_t) \end{aligned}$$

com $k_t \in \mathbb{N}$ apropriado. Logo os valores $f(n_0 + t \cdot p) = p(1 + k_t)$ com $t \in \mathbb{N}$ são compostos. Como $k_t = a_s p^s t^s \pm ...$, assume infinitos valores naturais distintos quando $t \in \mathbb{N}$, concluímos nossa demonstração. □

CAPÍTULO

5

SOBRE O ÚLTIMO TEOREMA DE FERMAT

Neste capítulo, apresentamos a história do Último Teorema de Fermat e, em seguida, dois casos particulares desse teorema. Especificamente, mostramos que a equação $x^n + y^n = z^n$ não possui solução para o caso $n = 4$ e o caso n=3. As seções a seguir podem ser lidas em qualquer ordem. No entanto, apresentamos primeiro a história do Último Teorema de Fermat, para que seja uma motivação para o estudo de casos particulares desse teorema, apresentados em seguida.

5.1 A história do Último Teorema de Fermat

A história do Último Teorema de Fermat está fortemente ligada à história da matemática e se relaciona com quase todos os temas da teoria dos números. Como veremos, essa história tem origem com Pitágoras, na Grécia antiga, em torno de dois mil anos antes de Pierre de Fermat criar o problema como é conhecido hoje. Além disso, esse teorema foi provado, efetivamente, somente em 1994 pelo matemático Andrew Wiles e publicado em 1995. Assim, esse teorema une a matemática criada por Pitágoras às ideias mais sofisticadas da matemática moderna.

Especificamente, o Último Teorema de Fermat afirma que não existe solução em números inteiros para a equação

$$x^n + y^n = z^n,$$

para $n > 2$. Um dos pontos mais interessantes desse problema é que ele tem uma apresentação simples, diferente de muitos outros problemas de matemática, em que grande parte da dificuldade consiste em entender a questão colocada por eles. Além disso, é um problema que apresenta uma certa familiaridade, pois é baseado num elemento de matemática que todos conhecem, o teorema de Pitágoras, que diz que num triângulo retângulo o quadrado da hipotenusa é igual à soma dos quadrados dos catetos, ou seja, $x^2 + y^2 = z^2$.

No século VI a.C. Pitágoras de Samos foi um dos matemáticos mais influentes da época. Ele desenvolveu a ideia da lógica matemática e foi responsável pela primeira idade de ouro da

matemática. Suas habilidades matemáticas foram adquiridas em suas viagens pelo mundo antigo e aprendeu muitas técnicas matemáticas com os egípcios e babilônios. Dentre suas práticas voltadas para o estudo e disseminação da matemática, Pitágoras fundou a chamada Irmandade Pitagórica, um grupo de seguidores para o qual ele podia passar seus ensinamentos e que podia também contribuir criando novas ideias matemáticas. Mas além de estudar as relações entre os números, Pitágoras se interessava intensamente pela ligação entre os números e a natureza. Ele percebeu que os fenômenos naturais são governados por leis que podem ser descritas por equações matemáticas. Uma das primeiras ligações que ele percebeu foi a relação fundamental entre a harmonia da música e a harmonia dos números. Assim, ele descobriu pela primeira vez as leis matemáticas que governam um fenômeno físico e demonstrou uma relação fundamental entre a matemática e a ciência. A partir dessa e de outras descobertas Pitágoras percebeu que os números estavam ocultos em tudo, das harmonias da música até as órbitas dos planetas, o que o levou a proclamar que "tudo é número". De todas as ligações entre os números e a natureza estudadas por Pitágoras e a Irmandade Pitagórica, a mais importante é a relação que leva o nome do próprio Pitágoras. O Teorema de Pitágoras apresenta uma equação que é verdadeira para todos os triângulos retângulos e que, portanto, também define o ângulo reto. Mas o ângulo reto, por sua vez, define a perpendicular e a perpendicular define as dimensões (comprimento, largura e altura) do espaço em que vivemos. Logo, podemos ver que a matemática, através do triângulo retângulo, define a própria estrutura do nosso mundo tridimensional. Essa foi uma descoberta profunda, mas a matemática para compreender o Teorema de Pitágoras é relativamente simples e o motivo pelo qual o teorema leva o nome de Pitágoras é que ele foi o primeiro a demonstrar esse resultado. Em suma, o Teorema de Pitágoras foi um marco na história da matemática e um dos saltos mais importantes da história da civilização. E a importância dessa descoberta está, basicamente, em dois sentidos. Em primeiro lugar, ela desenvolveu a ideia de prova (ou demonstração) de um resultado matemático. E em segundo lugar, como visto acima, o Teorema de Pitágoras liga um método matemático abstrato a alguma coisa tangível.

Pitágoras e seus "discípulos" chamavam de *trios pitagóricos* às combinações de três números inteiros que satisfaçam à equação de Pitágoras $x^2 + y^2 = z^2$, e encontrar os trios pitagóricos é relativamente fácil. No entanto, ao mudar a potência de 2 para 3, encontrar números inteiros que satisfaçam a equação cúbica $x^3 + y^3 = z^3$ parece impossível. Além disso, se a potência for mudada de 3 para qualquer número mais alto $n \geq 4$, a descoberta de uma solução também parece impossível. Ou seja, parecem não existir soluções para a equação mais geral

$$x^n + y^n = z^n, \quad n > 2.$$

Assim, ao simplesmente trocar o 2 da equação de Pitágoras por qualquer número maior, a busca por soluções das equações deixa de ser um problema relativamente simples e se torna um desafio que parece impossível. E Pierre de Fermat tinha certeza de que não existiam inteiros que solucionassem a equação, "com base em uma demonstração".

Depois da morte de Pitágoras (por volta de 510 a.C.), a ideia da demonstração matemática

se espalhou rapidamente pelo mundo civilizado e no ano 332 a.C., depois de conquistar a Grécia, a Ásia Menor e o Egito, Alexandre, o Grande, decidiu construir uma capital que seria a cidade mais imponente do mundo e se tornaria um importante centro de estudos. De fato, após a morte de Alexandre, quando Ptolomeu I subiu ao trono do Egito, Alexandria se tornou o local da primeira universidade do mundo. Matemáticos e outros intelectuais emigraram para a cidade atraídos também pela reputação da universidade, mas principalmente pela Biblioteca de Alexandria.

A ideia da Biblioteta foi de Demétrio Falero, um orador impopular, que foi forçado a deixar Atenas e encontrou asilo em Alexandria. Ele convenceu Ptolomeu a reunir todos os grandes livros, assegurando-lhe que as grandes mentes viriam atrás deles. Depois que os volumes do Egito e da Grécia foram colocados na Biblioteca, agentes vasculharam a Europa e a Ásia Menor em busca de outros volumes de conhecimentos. Até mesmo os viajantes que chegavam em Alexandria não escapavam da fiscalização para alimentar a Biblioteca. Quando chegavam na cidade, seus livros eram confiscados e levados aos escribas. Então, os livros eram copiados de modo que, enquanto o original ia para a Biblioteca, uma duplicata era dada ao dono. Dessa forma, depois de algum tempo a Biblioteca continha cerca de 600 mil livros e os matemáticos podiam absorver todo o conhecimento do mundo estudando em Alexandria.

O primeiro diretor do departamento de matemática da universidade de Alexandria foi Euclides. Euclides nasceu em 330 a.C. e acreditava, como Pitágoras, na busca pela matemática pura e não buscava aplicações para o seu trabalho. Ele dedicou boa parte da sua vida escrevendo os *Elementos*, o livro-texto mais bem-sucedido de toda a história. Os *Elementos* consistem em treze livros, alguns dedicados aos trabalhos do próprio Euclides, e os outros sendo uma compilação do conhecimento matemático de sua época, incluindo dois volumes dedicados inteiramente aos trabalhos da Irmandade Pitagórica. Nos séculos a partir de Pitágoras, os matemáticos tinham inventado muitas técnicas lógicas que podiam ser aplicadas em diferentes circunstâncias e Euclides teve a habilidade de usar todas elas nos *Elementos*. Em particular, ele explorou a técnica conhecida como prova por absurdo ou prova por contradição. Ao usar a prova por contradição, Euclides pôde provar a existência dos números irracionais e pela primeira vez os números adquiriam uma qualidade nova e mais abstrata. É interessante observar que, para Pitágoras, a beleza da matemática era a ideia de que os números racionais poderiam explicar todos os fenômenos naturais. Esta filosofia fez com que Pitágoras se negasse a aceitar a existência dos números irracionais e isto é considerado como o ato mais vergonhoso e, talvez, a maior tragédia da matemática grega.

Embora Euclides se interessasse muito pela teoria dos números, sua maior contribuição para a matemática foi na geometria. De fato, os *Elementos* foram a base do ensino de geometria nas escolas e universidades durante dois mil anos após suas publicações. O matemático que escreveu um livro equivalente, sobre a teoria dos números, foi Diofante de Alexandria que, embora suas realizações estejam bem documentadas, quase nada se sabe sobre sua vida. Acredita-se que ele tenha vivido em torno do ano 250. Diofante gostava de resolver problemas que exigiam

soluções com números inteiros e, de fato, atualmente estes problemas são conhecidos como problemas de Diofante. Sua carreira foi desenvolvida em Alexandria e ele reuniu muitos dos problemas em que trabalhou em seu tratado, intitulado *Aritmética*. A *Aritmética* de Diofante foi dividida em 13 volumes e foram alguns desses que inspiraram matemáticos, como Pierre de Fermat.

Pierre de Fermat nasceu em 1601, na cidade de Beaumont-de-Lomagne, no sudoeste da França. Ele recebeu uma educação privilegiada no monastério franciscano de Grandselve e em seguida na Universidade de Toulouse. Não existem registros de que Fermat mostrasse qualquer talento especial para a matemática e, pela pressão de sua família, ele se dedicou ao serviço público. Em 1631 foi nomeado *conseiller au Parlement de Toulouse*, conselheiro na Câmara de Requerimentos. Fermat foi um servidor público eficiente e teve uma ascensão rápida em sua carreira, tornando-se membro da elite, o que lhe permitia usar o *de* como parte do seu nome. No tempo que lhe sobrava, Fermat se dedicava à matemática. Ele era um verdadeiro estudioso amador, mas era tão talentoso que, quando Julian Coolidge escreveu sua *Matemática dos grandes amadores*, ele excluiu Fermat, dizendo que "fora tão grande que devia ser considerado profissional".

No início do século XVII, a matemática ainda se recuperava da Idade das Trevas, época (entre 389 e 642) em que alguns conflitos, especialmente religiosos, destruíram grande parte da Biblioteca de Alexandria e a matemática no Ocidente ficou reduzida ao básico e, por isso, é verdade dizer que a maioria dos matemáticos do século XVII eram amadores. Vivendo longe de Paris, Fermat estava isolado da pequena comunidade matemática que lá existia. Faziam parte dessa comunidade nomes como Pascal, Gassendi, Roberval , Beaugrand e o padre Mersenne.

O padre Mersenne fez poucos avanços na matemática, mas ele desempenhou um papel muito importante nessa ciência no século XVII. Quando chegou em Paris, ele estava determinado a encorajar os matemáticos a trocarem ideias e aperfeiçoar os trabalhos uns dos outros. Em particular, ele organizou encontros regulares e seu grupo formou o núcleo do que seria a Academia Francesa. Mersenne também viajou pela França e pelo exterior divulgando as últimas descobertas na matemática. Em suas viagens ele se encontrou com Pierre de Fermat e acabou se tornando uma influência significativa sobre Fermat. No entanto, apesar de seus esforços, Fermat se recusava a revelar suas demonstrações. A publicação e o reconhecimento público nada significavam para ele, ficando satisfeito em somente criar novos teoremas sem ser perturbado. Contudo ele parecia se divertir escrevendo cartas para outros matemáticos, enunciando seus teoremas sem fornecer as demonstrações, como uma espécie de provocação.

Fermat é considerado um dos responsáveis pelo desenvolvimento da teoria da probabilidade e do cálculo e isto seria mais do que suficiente para que ele fosse considerado um dos mais importantes matemáticos da história. Mas, sua grande paixão era por um assunto geralmente inútil, *a teoria dos números* e foram aí suas maiores realizações. Fermat era obcecado em entender as propriedades e relações entre os números. Essa é a forma mais pura e antiga da

matemática, e Fermat estava ampliando um conhecimento que fora iniciado por Pitágoras.

Não há registros de que o interesse de Fermat pela matemática tenha sido influenciado por algum tipo de tutor, mas sim por uma cópia da *Aritmética*. Em um único livro da *Aritmética* Fermat podia encontrar todo o conhecimento dos números obtidos por gênios como Pitágoras e Euclides. A *Aritmética* continha mais de cem problemas e, para cada um Diofante dava uma solução detalhada, diferente de Fermat que não estava interessado em escrever um livro-texto para as gerações futuras. Enquanto estudava os problemas e as soluções de Diofante, Fermat era levado a pensar em outros problemas mais sutis e enfrentá-los, anotando, às vezes, comentários e fórmulas nas margens de sua cópia da *Aritmética*. Essas notas se tornariam registros valiosos dos mais brilhantes cálculos de Fermat.

O mais famoso problema de Fermat foi um desafio para o resto do mundo. Enquanto estudava o Livro II da *Aritmética*, Fermat encontrou vários problemas e soluções relacionados com o teorema de Pitágoras e os trios pitagóricos. Então, começou a brincar com a equação de Pitágoras tentando descobrir alguma coisa que escapara à atenção do gregos. E, num instante de genialidade que o imortalizaria, ele encontrou uma equação que, embora fosse muito semelhante à de Pitágoras, não tinha solução. Como já mencionamos, ao invés de considerar a equação $x^2+y^2=z^2$, Fermat se concentrou na equação $x^3+y^3=z^3$, uma variante da equação de Pitágoras e percebeu que essa nova equação parecia não ter solução inteira. Fermat alterou ainda mais a equação de Pitágoras trocando a potência para números maiores do que 3 e descobriu que a busca por soluções inteiras para estas equações era igualmente difícil. De acordo com Fermat, parecia não existir um trio de números inteiros que satisfizesse a equação

$$x^n+y^n=z^n, \quad n\geq 3.$$

Na margem de sua *Aritmética*, Fermat escreveu uma nota de sua observação: "*É impossível para um cubo ser escrito como a soma de dois cubos ou uma quarta potência ser escrita como uma soma de dois números elevados a quatro, ou, em geral, para qualquer número que seja elevado a uma potência maior do que dois ser escrito como a soma de duas potências semelhantes.*" E depois desta primeira nota, em que esboça sua teoria, ele fez um comentário adicional que perturbaria gerações de matemáticos: "***Eu tenho uma demonstração realmente maravilhosa para esta proposição, mas esta margem é muito estreita para contê-la.***".

Este era Fermat no seu modo mais frustrante. Suas palavras mostram que ele estava satisfeito com sua demonstração, mas não se daria ao trabalho de escrevê-la em detalhes, quanto menos publicá-la. Ele nunca falou a ninguém sobre sua prova e, no entanto, apesar dessa combinação de desinteresse em compartilhar e modéstia, o Último Teorema de Fermat, como mais tarde seria chamado, se tornaria famoso no mundo todo pelos séculos seguintes.

A descoberta de Fermat ocorreu por volta de 1637. Trinta anos depois ele ficou seriamente doente e morreu em 9 de janeiro de 1665. Felizmente, seu filho mais velho Clément-Samuel, percebia a importância do "*hobby*" de seu pai e decidiu que aquelas descobertas não seriam

esquecidas. Clément-Samuel passou cinco anos reunindo e examinando cartas e anotações de seu pai nas margens de sua cópia da *Aritmética* e ele publicou estas anotações em uma edição especial da *Aritmética*. Em 1670, em Toulouse, ele apresentou sua *Aritmética de Diofante contendo observações de P. de Fermat* que, ao lado do tradicional grego e da tradução de Bachet estavam quarenta e oito observações feitas por Fermat.

Depois que a *Observações* de Fermat chegara à comunidade matemática, ficou claro que as cartas que ele tinha enviado para seus colegas, incluindo padre Mersenne, eram pouco, perto de todas as suas descobertas. Suas notas pessoais continham vários teoremas importantes. No entanto, não eram acompanhados por nenhuma explicação, ou tinham apenas ideias da demonstração. Mas seus resultados apresentavam uma lógica tão boa que os matemáticos não tiveram dúvidas de que Fermat realmente tivera as demonstrações. Logo, recriar essas demonstrações seria um desafio para eles.

À medida que os séculos passavam, todas as observações foram sendo demonstradas, mas nenhum matemático conseguia demonstrar o Último Teorema de Fermat. De fato, ele é conhecido como o "Último" Teorema, porque foi a última observação por ser demonstrada, passando pelas mãos de muitos matemáticos em torno de trezentos anos sem que pudesses ser resolvido. No entanto, várias tentativas no intuito de resolver o problema foram criando o caminho para que ele fosse finalmente resolvido.

Leonhard Euler foi quem fez o primeiro avanço em direção à prova do Último Teorema de Fermat. Euler imaginou se não poderia provar que uma das equações não tinha solução e então obter o mesmo resultado para todas as outras equações restantes, ou seja, utilizando o método de indução infinita. Então, inicialmente ele deveria provar o resultado para o caso $n = 3$. E para isto ele pôde contar com uma pista oculta nas anotações de Fermat em que ele descreveu, disfarçadamente, uma prova para o caso $n = 4$ em outra parte de sua *Aritmética* para demonstrar um um problema totalmente diferente. Resumidamente, ele assumiu que existia uma solução para a equação $x^4 + y^4 = z^4$ e mostrou que, então, deveria existir uma solução menor e, ao analisar esta solução menor, deveria existir outra ainda menor e assim por diante, gerando infinitas soluções de forma decrescente. Mas isto seria uma contradição, pois como x, y, z devem ser números inteiros, deveria existir uma menor solução possível. Esta prova por contradição é conhecida como *método da descida infinita*.

Em 04 de agosto de 1753, Euler divulgou que havia adaptado o método da descida infinita de Fermat e conseguira demonstrar, com sucesso, o caso $n = 3$. Depois de cem anos esta era a primeira vez que alguém conseguia fazer algum avanço na direção de solucionar o desafio de Fermat. Mas, para fazer com que a prova de Fermat para $n = 4$ cobrisse também o caso $n = 3$, Euler teve que incorporar em sua demonstração o conceito de *números imaginários*. Os números imaginários acrescentam uma nova dimensão à matemática e Euler esperava poder explorar este grau de liberdade para atacar o Último Teorema de Fermat. No entanto, apesar de sua grande realização para o caso $n = 3$, Euler não pôde repetir o método para os outros casos englobados

pelo Último Teorema de Fermat.

Assim, cem anos depois da morte de Fermat, existiam demonstrações para apenas para os casos $n = 3$ e $n = 4$ do Último Teorema de Fermat. Mas, embora o progresso feito nesses cem anos fosse lento, a situação não era tão ruim quanto parecia, pois a demonstração para o caso $n = 4$ também serve de prova para os números que são múltiplos de 4. E, pelo mesmo argumento, a demonstração de Euler para $n = 3$ automaticamente serve de prova para os números que são múltiplos de 3. Logo, para demonstrar o Teorema de Fermat para todos os valores de n basta prová-lo para valores primos de n, pois todos os outros casos serão múltiplos dos casos primos e serão provados implicitamente. Dessa forma, o problema deveria se tornar mais simples, se não fosse o detalhe de que a quantidade de números primos é infinita.

No começo do século XIX, o Último Teorema de Fermat já era conhecido como o mais famoso problema da teoria dos números. Desde o avanço realizado por Euler não houvera mais progressos, mas uma revelação, feita por uma jovem francesa, iria dar força pela busca de uma demonstração. Shophie Germain viveu em uma época de preconceitos intelectuais relacionados às mulheres e, para realizar suas pesquisas, ela foi obrigada a assumir uma identidade falsa, estudar em condições terríveis e trabalhar em isolamento intelectual. Ainda assim, ela conseguiu se firmar como uma grande teórica dos números e revolucionou o estudo do Último Teorema de Fermat, fazendo uma contribuição ainda maior do que todos os homens que a antecederam.

Desde a demonstração de Euler, os matemáticos vinham tentando demonstrações para casos particulares do Último Teorema de Fermat. Contudo, Sophie adotara uma nova estratégia em que descreve a chamada abordagem geral para o problema. O seu objetivo não era provar um caso particular, mas dizer algo sobre muitos casos de uma só vez. Então, em uma carta para o matemático Carl Gauss, ela desenvolveu um argumento elegante para demonstrar que provavelmente não existem soluções para $x^n + y^n = z^n$ para valores de n iguais a primos p tais que $2p + 1$ também seja primo.

Em 1825 o método de Shophie Germain teve seu primeiro sucesso. De forma independente, os matemáticos Gustav Lejeune-Dirichilet e Adrien-Marie Legendre provaram que o caso $n = 5$ não tinham solução baseando suas provas no trabalho de Shophie Germain. E quatorze anos depois, Gabriel Lamé fez alguns acréscimos engenhosos ao método de Germain e conseguiu a demonstração para o caso $n = 7$.

Depois da descoberta de Shophie Germain, a Academia Francesa de Ciências ofereceu uma série de prêmios, incluindo uma medalha de ouro e três mil francos, ao matemático que pudesse finalmente demonstrar e terminar com o mistério do Último Teorema de Fermat. Então, no dia 1^o de março de 1847, a Academia teve a reunião mais dramática de sua história. Gabriel Lamé, que havia demonstrado o caso $n = 7$ alguns anos antes, anunciou que tinha quase pronta uma demonstração, delineou seu método e previu que dentro das próximas semanas publicaria a demonstração completa no jornal da Academia. No entanto, nessa mesma reunião, Augustin Louis Cauchy, outro dos melhores matemáticos de Paris, anunciou à Academia que estivera

trabalhando numa abordagem semelhante à de Lamé, e que também estava próximo de publicar uma demonstração completa.

Cauchy e Lamé perceberam que a questão do tempo se tornara crucial e, três semanas depois do anúncio, eles depositaram envelopes lacrados no cofre da Academia. Esta era uma prática comum naquela época, que permitia aos matemáticos fazerem um registro sem revelar os detalhes de seu trabalho. Se mais tarde surgisse uma disputa quanto à originalidade das ideias, os envelopes lacrados dariam a evidência para estabelecer a prioridade.

Em abril a expectativa aumentou quando Cauchy e Lamé publicaram detalhes vagos, mas fascinantes de suas demonstrações. Mas em 24 de maio Joseph Liouville chocou a audiência da Academia quando leu uma carta do matemático alemão Ernest Kummer, um dos melhores teóricos dos números de todo o mundo. Para Kummer ficou óbvio que os dois franceses estavam caminhando para um mesmo erro e delineou seu ponto de vista na carta que enviara para Liouville. De acordo com Kummer, o problema fundamental era que as duas demonstrações dependiam do uso de uma propriedade dos números conhecida como fatoração única e ambas as demonstrações envolviam números imaginários. E, embora a fatoração única seja verdadeira para números reais, ela pode se tornar falsa para números imaginários. Assim, Kummer havia mostrado que a demonstração completa do Último Teorema de Fermat estava além de abordagens com a matemática da época.

Depois do trabalho de Kummer, as esperanças de se descobrir uma demonstração para o Último Teorema de Fermat pareciam cada vez menores. Além disso, em 1903 o matemático Kurt G*ö*del publicou um trabalho que desanimaria ainda mais os matemáticos que tinham esperança em demonstrar o Último Teorema. Nesse trabalho G*ö*del desenvolveu uma teoria que continha os chamados teoremas da indecidibilidade que, de forma resumida, diziam que alguns problemas matemáticos poderiam ser impossíveis de solucionar. E esta ideia se aplicaria sobre o Último Teorema de Fermat, ou seja, talvez este teorema fosse indecidível.

No entanto, haviam matemáticos que ainda lutavam com o Último Teorema de Fermat e, com a chegada dos computadores, começaram a atacar os casos mais difíceis do Último Teorema de Fermat que, com esta nova ferramenta, podiam então ser enfrentados com mais rapidez. Depois da Segunda Guerra Mundial, equipes de matemáticos e cientistas dos computadores demonstraram o Último Teorema de Fermat para valores de n até 500, depois para valores até 1.000 e 10.000. Na década de 1980, o limite foi elevado para 25.000 e, mais recentemente, os matemáticos já podiam afirmar que o Último Teorema de Fermat era verdadeiro para todos os valores de n até 4 milhões. No entanto, mesmo que os computadores passassem décadas demonstrando um valor de n depois do outro, eles nunca poderiam demonstrar todos os valores de n até o infinito e, assim, nunca poderiam demonstrar todo o teorema. Logo, tudo o que os computadores poderiam oferecer eram evidências de que o Último Teorema de Fermat era verdadeiro. Mas, este já era um bom motivo para que os matemáticos voltassem a se animar para a busca de uma demonstração.

Em 1954, um jovem matemático chamado Goro Shimura, da Universidade de Tóquio, foi à biblioteca de seu departamento para emprestar um artigo que precisava sobre a teoria algébrica da multiplicação complexa, para ajudá-o em um cálculo difícil de um de seus trabalhos. No entanto, o artigo havia sido emprestado para um outro matemático, Yutaka Taniyama, conhecido ocasional de Shimura. Então Shimura, escreveu para Taniyama explicando que precisava urgentemente do artigo para completar um cálculo difícil e, educadamente perguntou quando ele seria devolvido. Alguns dias depois Shimura recebeu uma carta de Taniyama dizendo que ele estava trabalhando exatamente no mesmo cálculo e que estava preso no mesmo ponto da lógica. E sugeriu que eles compartilhassem suas ideias para tentarem solucionar o problema em conjunto. Esse encontro casual em torno de um artigo emprestado pela biblioteca deu início a uma parceria que mudaria o curso da história da matemática e, de forma especial, do Último Teorema de Fermat.

Um tópico, particularmente fora de moda, que fascinava Taniyama e Shimura era o estudo das *formas modulares*. O fator principal das formas modulares é seu nível excessivo de simetria. Lembrando que, em matemática, um objeto tem "simetria" se ele puder ser transformado de um modo especial (como, por exemplo, rotação, reflexão e translação) e depois disso permanecer o mesmo. Um exemplo muito simples que podemos citar é o caso de um quadrado, que possui simetria rotacional e se tivermos infinitos quadrados adjacentes no plano, também temos a simetria reflexiva.

As formas modulares estudadas por Taniyama e Shimura podem ser empurradas, trocadas, refletidas e giradas um número infinito de modos que ainda permanecerão imutáveis, o que as torna os objetos matemáticos mais simétricos que existem. Infelizmente, é impossível desenhar ou imaginar uma forma modular.

Um outro interesse de Taniyama e Shimura era o estudo das *equações elípticas*, que são equações da forma

$$y^2 = x^3 + ax^2 + bx + c,$$

onde a, b e c são números inteiros. Elas recebem este nome, porque no passado eram usadas para medir o perímetro de elipses e os comprimentos das órbitas dos planetas. O desafio das equações elípticas, assim como no caso do Último Teorema de Fermat, é determinar se elas possuem soluções para números inteiros e, se assim for, quantas soluções existem.

Formas modulares e equações elípticas fazem parte de áreas completamente diferentes na matemática e, ninguém acreditaria que poderia existir alguma relação remota entre os dois assuntos. Contudo Taniyama e Shimura chocaram a comunidade matemática ao sugerirem que as equações elípticas e as formas modulares eram na verdade uma coisa só. De acordo com esses matemáticos, seria possível unificar os mundos modulares e elípticos, ou seja, toda equação elíptica deveria se relacionar com uma forma modular. As evidências apresentadas por Taniyama e Shimura eram tão fortes que fizeram com que essa teoria fosse cada vez mais aceita, recebendo o nome de conjectura.

No outono de 1984 um grupo de teóricos dos números se reuniu para um simpósio em Oberwolfach, uma pequena cidade da Alemanha. Eles tinham se reunido para discutir várias descobertas no estudo das equações elípticas e, ocasionalmente, apresentavam pequenos progressos feitos na direção da prova do conjectura de Taniyama-Shimura. Um dos participantes desse encontro era Gerhard Frey, um matemático de Saarbrücken. Ele não tinha nenhuma ideia nova sobre como abordar a conjectura, mas fez a surpreendente afirmação de que se a conjectura de Taniyama-Shimura fosse provada, então o Último Teorema de Fermat também seria imediatamente provado e vice-versa. Ou seja, o Último Teorema de Fermat seria verdadeiro se, e somente se, a conjectura de Taniyama-Shimura fosse verdadeira. No entanto, apesar de todos ficarem impressionados com a afirmação de Frey, eles perceberam um erro crucial em sua lógica. O erro não parecia ser sério, mas tornava o trabalho de Frey incompleto. Quem conseguisse corrigir esse erro receberia o crédito por ligar a conjectura de Taniyama-Shimura ao Último Teorema de Fermat.

Muitos matemáticos tentaram completar a ligação entre a conjectura de Taniyama-Shimura e o Último Teorema de Fermat, mas foi Ken Ribet, um professor da Universidade da Califórnia em Berkeley quem conseguiu fazer a descoberta crucial. Agora sim, o problema mais importante do século XVII fora ligado ao problema mais significativo do século XX. Contudo, mesmo Ribet era pessimista em acreditar que a conjectura de Taniyama-Shimura pudesse ser provada. Ele nunca imaginaria que estaria no auditório, alguns anos mais tarde, quando essa demonstração fosse apresentada pelo matemático Andrew Wiles.

Andrew Wiles nasceu e cresceu em Cambrigde e foi lá que conheceu o problema que dominaria o resto de sua vida. Em 1963, aos dez anos de idade, Wiles já gostava e se identificava muito com a matemática. Um dia, quando voltava para casa, da escola ele decidiu passar em uma biblioteca. Era uma biblioteca pequena, mas tinha uma boa coleção de livros sobre enigmas e isso atraía a atenção de Wiles. Em geral, eram livros que continham problemas de matemática e, para cada problema havia uma solução apresentada nas últimas páginas. Mas naquele dia Andrew foi atraído por um livro que tinha apenas um problema e nenhuma solução.

O livro se chamava *O último problema*, de Eric Temple Bell. Ele apresentava a história do Último Teorema de Fermat, um problema matemático que tinha suas origens na Grécia antiga, mas só atingira sua maturidade no século XVII, quando o matemático francês Pierre de Fermat o colocara como um desafio para o resto do mundo. Um problema que durante trezentos anos ninguém conseguira uma solução.

O que mais fascinou Wiles, foi a simplicidade da apresentação do problema. Ele, com dez anos podia entender a questão colocada pelo problema e, no entanto, nenhum dos grandes matemáticos da história conseguira resolvê-lo. A partir daquele momento, Wiles não desistiria de tentar solucionar o desafio deixado por Fermat e, desde então, começou a trabalhar no problema, usando todas as técnicas em seus livros escolares para tentar recriar a demonstração. Ele acreditava que talvez pudesse perceber alguma coisa que todos os outros, exceto Fermat

tinham deixado passar despercebido.

Em 1975, Andrew Wiles começou seus estudos como estudante de pós-graduação na Universidade de Cambridge e teve como orientador o australiano John Coates, professor no Emmanuel College, originalmente de Possum Brush, Nova Gales do Sul. Desde o início dessa orientação, Coats reconhecia que Wiles, apesar de ainda ser estudante, tinha ideias muito profundas e acreditava que iria ser um grande matemático.

Nessa época, Wiles teve que deixar um pouco Fermat de lado, pois precisaria se dedicar aos seus estudos e, além disso, percebeu que as únicas técnicas para lidar com o problema tinham mais de 130 anos e não lhe parecia que estas técnicas estavam chegando na raiz do problema. No entanto, apesar da dificuldade não pensava em desistir, pois acreditava que valia a pena trabalhar em qualquer problema, desde que ele gere matemática interessante ao longo do caminho.

Então, John Coats decidiu que Wiles deveria estudar as *equações elípticas*. As equações elípticas foram originalmente estudadas pelos matemáticos gregos, incluindo Diofante, que dedicou uma grande parte de sua *Aritmética* ao estudo de suas propriedades. Provavelmente inspirado por Diofante, Fermat também estudou as equações elípticas. Logo, como elas tinham sido estudadas por seu herói, Wiles ficou feliz de poder explorá-las ainda mais. E esta decisão seria um ponto vital para a carreira de Wiles e lhe daria as técnicas necessárias para uma nova abordagem do Último Teorema de Fermat.

Trabalhando junto com John Coats, Wiles rapidamente estabeleceu sua reputação como um brilhante teórico dos números, um matemático dotado de uma compreensão profunda sobre as equações elípticas. Contudo, à medida que chegava a um novo resultado e publicava mais um trabalho, Wiles não percebia que, de fato, estava reunindo a experiência que o levaria, alguns anos depois, à demonstração do Último Teorema de Fermat.

Embora ninguém estivesse ciente disso, nessa ocasião a matemática japonesa já tinha iniciado os estudos que ligariam as equações elípticas ao Último Teorema de Fermat, através da conjectura de Taniyama-Shimura, como já foi descrito acima.

Depois de completar seu ph.D. com o professor John Coats, em Cambridge, Andrew Wiles se mudou para os Estados Unidos e assumiu como professor na Universidade de Princeton, onde conquistou a reputação de ser um dos matemáticos mais talentosos de sua geração. E numa tarde, no final do verão de 1986, quando estava tomando chá na casa de um amigo, Wiles soube que Ken Ribet havia demonstrado a ligação entre a conjectura de Taniyama-Shimura e o Último Teorema de Fermat. Ele não podia acreditar. Naquele momento ele sabia que o rumo de sua vida estava mudando, pois isto significava que para demonstrar o Último Teorema de Fermat ele só precisaria demonstrar a conjectura de Taniyama-Shimura. Ou seja, tinha que provar que cada equação elíptica estava relacionada com uma forma modular. Wiles sabia que iria para casa e começaria a trabalhar na conjectura de Taniyama-Shimura.

Duas décadas tinham se passado desde que Andrew Wiles descobrira o livro, na biblioteca,

que o inspirara a aceitar o desafio de Fermat, mas agora pela primeira vez, ele podia ver o caminho em direção ao sonho de sua infância. Graças à orientação de Coats, Wiles era, provavelmente, a pessoa que mais sabia sobre equações elípticas no mundo e, assim, apesar de saber que a tarefa que o aguardava era imensa, ele não teve dúvidas de que deveria tentar. Então, Wiles abandonou todos os trabalhos que não fossem relevantes para a demonstração do Último Teorema de Fermat e deixou de participar de muitas das atividades, como conferências e colóquios que antes participava. Ele continuou apenas a participar de seminários e dar aulas para os estudantes de graduação. Sempre que possível, evitava as distrações da faculdade, trabalhando em casa, onde se refugiava em seu estúdio no sótão. Lá ele procurava expandir o poder das técnicas estabelecidas, esperando desenvolver uma estratégia para seu ataque sobre a conjectura de Taniyama-Shimura.

Wiles tomou a decisão de trabalhar em completo isolamento e segredo. No entanto, os matemáticos modernos desenvolveram uma cultura de cooperação e colaboração e, assim, a decisão de Wiles parecia retornar a uma época anterior. Era como se estivesse imitando a abordagem do próprio Fermat, um dos mais famosos eremitas matemáticos. Mas, Wiles, em algumas oportunidades, explicou que parte do motivo de querer trabalhar em segredo estava em seu desejo de não ser distraído.

Depois de algum tempo, Wiles descobriu que, basicamente, o seu desafio era a técnica de *indução* para a sua demonstração. Ele precisaria construir um argumento indutivo para mostrar que cada uma das infinitas equações elípticas podia ser relacionada com cada uma das formas modulares.

Depois de sete anos de muito esforço e de criar uma teoria complexa em torno de seu problema, Wiles tinha completado a demonstração da conjectura de Taniyama-Shimura. E, consequentemente, depois de sonhar trinta anos, ele também demonstrara o Último Teorema de Fermat. Agora era hora de anunciar ao mundo a sua conquista.

Então, por volta de maio de 1993 ele estava convencido de que sua demonstração estava terminada e resolveu apresentá-la numa conferência que haveria em Cambridge no final de junho daquele ano. Cambridge era sua cidade natal e ele havia feito sua pós-graduação lá, então ele achou que não haveria melhor lugar para anunciar sua prova.

O título da conferência era “Funções L e Aritmética”, sendo voltada para palestras sobre teoria dos números e seria realizada no Instituto Isaac Newton. Um dos organizadores da conferência era o supervisor de Ph. D. de Wiles, John Coats. Além disso, participaram da conferência importantes personalidades da teoria dos números, incluindo Ken Ribet, que havia inspirado os sete anos de trabalho duro de Wiles.

Wiles precisou de três palestras para poder apresentar seu “resultado”. O título de suas palestras era “Formas Modulares, Curvas Elípticas e Representação de Galois”. Era um título vago, não dando pistas sobre o objetivo final das palestras. Mas, ainda assim, já haviam alguns boatos de que Wiles provaria o Último Teorema de Fermat.

A primeira palestra de Wiles foi aparentemente simples, estabelecendo apenas as bases para o seu ataque contra a conjectura de Taniyama-Shimura que seria na segunda e terceira palestras. A maioria das pessoas na plateia que não ouvira os boatos, não percebeu o objetivo da palestra e deu pouca atenção aos detalhes. Já os que sabiam, estavam buscando o menor indício que pudesse apoiar os rumores.

Logo depois que a palestra terminou, o boato voltou a circular e com mais vigor, e as mensagens circularam através do correio eletrônico. Um dos estudantes pós-graduados, que assistira à palestra, correu para uma loja de apostas tentando apostar dez libras como o Último Teorema de Fermat seria resolvido em uma semana. Contudo, a loja pressentiu o que estava acontecendo e se recusou a aceitar a aposta. Aquele era o terceiro matemático que procurava a loja naquele dia tentando fazer uma aposta semelhante.

No dia seguinte, mais pessoas haviam escutado os boatos e, então a plateia para a segunda palestra era bem maior. Wiles provocou a audiência com um cálculo intermediário, que mostrava claramente que ele estava tentando dominar a conjectura de Taniyama-Shimura. Mas todos continuavam na dúvida se ele tinha o suficiente para demonstrá-la e, consequentemente demonstrar o Último Teorema de Fermat.

No dia 23 de junho, Andrew começou sua terceira e última palestra e todas as pessoas que contribuíram para as ideias por trás de sua demonstração estavam na sala, em particular, Ken Ribet. A essa altura os boatos eram tão persistentes que todos na comunidade matemática apareceram para essa última palestra.

Depois de sete anos de esforços intensos, Wiles estava a ponto de apresentar ao mundo sua demonstração. Curiosamente Wiles diz não lembrar dos momentos finais da palestra com detalhes, mas que lembra do clima na sala:“Embora a imprensa já tivesse sido notificada do que estava acontecendo, não havia comparecido à palestra. Mas havia um bocado de gente na plateia que estava tirando fotos perto do final e o diretor do Instituto viera bem preparado, com uma garrafa de champanhe. Houve um silêncio respeitoso enquanto eu terminava a demonstração e encerrava com a declaração do Último Teorema de Fermat. Eu disse: ’Acho que vou parar por aqui’. E, então, houve um aplauso contínuo.”.

Todos que estavam naquela palestra tinham acabado de testemunhar um acontecimento histórico e mal podiam acreditar nisso, Wiles tinha solucionado um problema que durou cerca de 350 anos. No entanto, Wiles tinha sentimentos opostos sobre sua palestra. Se sentia, obviamente, feliz em ter solucionado um dos maiores problemas que a matemática já teve, mas também tinha um sentimento de perda, pois por muito tempo, parecia que aquele problema era apenas dele, era parte dele.

A palestra seguinte à de Wiles, foi justamente de Ken Ribet e ele relata como foi esta palestra da seguinte forma. “Eu dei a palestra, algumas pessoas tomaram notas, outras aplaudiram, e nenhum dos presentes, nem mesmo eu, tem ideia do que eu disse naquela palestra.”

Equipes de televisão e jornalistas científicos foram ao Instituto Newton para entrevistar "o maior matemático do século". A matemática chegava nas primeiras páginas dos jornais e, do dia para a noite, Wiles se tornou o matemático mais famoso do mundo. No entanto, enquanto os meios de comunicação estavam com a atenção voltada para o grande acontecimento na história da matemática, o trabalho sério de verificação da demonstração já começara. A demonstração de Wiles tinha que ser submetida a um exame de avaliação e ele teria que passar o verão esperando pela opinião dos avaliadores e sua aprovação.

Wiles submeteu seu trabalho à revista *Inventiones Mathematicae* e seu editor, Barry Mazur, começou o processo de selecionar os juízes para julgarem o trabalho. A demonstração de Wiles envolvia uma variedade tão grande de técnicas matemáticas, antigas e modernas, que Mazur tomou a decisão de nomear não apenas dois ou três examinadores, como é normal, mas seis. Para simplificar, as duzentas páginas da demonstração foram divididas em seis seções e cada um dos juízes assumiu a responsabilidade por um desses capítulos.

Às vezes, quando não podiam entender alguma parte da demonstração, os juízes enviavam um e-mail para Wiles com uma pergunta. Em geral, Wiles respondia os e-mails no mesmo dia ou no dia seguinte. Essas perguntas continuaram sem problemas até agosto daquele ano. Especificamente, em 23 de agosto, um dos juízes, Nick Katz, mandou um e-mail para Andrew, com uma pergunta que parecia um pouco mais complicada. Wiles enviou a Katz em torno de dois fax com explicações sobre o problema, mas nenhum deles satisfizeram Katz. Wiles presumiu que fosse um pequeno erro, como os outros, mas a persistência de Katz o forçou a levá-lo a sério. E, em setembro, ele começou a perceber que aquela não era uma pequena dificuldade, mas uma falha fundamental. O erro era tão abstrato que não poderia ser descrito em termos simples.

O erro encontrado não significava, necessariamente, que o trabalho de Wiles não pudesse ser salvo, mas significava que ele teria que reforçar sua demonstração. No entanto, Wiles decidiu fazer um esforço concentrado para concertar a falha de forma confidencial. Naquele momento somente os juízes e ele sabiam do erro. Então, ele resolveu voltar à rotina de se desligar completamente do mundo. Ele precisava se concentrar novamente, mas desta vez sob circunstâncias muito mais difíceis. Por um tempo ele achou que a solução estava bem próxima, que só estava deixando escapar algo simples e que tudo se encaixaria no dia seguinte. Mas à medida que o tempo passava o problema só se tornava mais difícil. Ainda assim, ele tinha a esperança de corrigir o erro antes que a comunidade matemática percebesse que o erro tinha existido.

A esposa de Wiles, que passara os sete anos ao seu lado, vendo os sete anos de esforços até à conquista daquela demonstração, tinha que ver agora a luta agonizante de seu marido contra um erro que poderia destruir todo seu trabalho. Mas ela acreditava mais do que qualquer um em Wiles e, como uma forma de incentivo, em setembro ela disse a ele que o único presente que queria de aniversário era a demonstração correta. O aniversário dela era em 6 de outubro. Ele tinha em torno de duas semanas para completar a prova, mas não conseguiu. De fato, o outono

passou e Wiles não pôde concertar o erro e, consequentemente, nenhum manuscrito sobre sua demonstração foi produzido. Assim os boatos começaram a circular e isto era um problema.

Wiles ainda tentou mais um pouco, mas sem sucesso, chegou à conclusão de que não poderia manter silêncio para sempre. A solução do erro não seria tão rápida. Então, depois de um outono desanimador, ele enviou um e-mail para o quadro de informações do Departamento de Matemática, explicando toda a situação. Mas nesse e-mail enfatizou de que acreditava que seria capaz de terminar a demonstração num futuro próximo, utilizando as ideias apresentadas em suas palestras em Cambridge. E prometeu que, por volta de fevereiro, faria um relato completo de seu trabalho.

Poucos acreditavam no otimismo de Wiles. Já tinham se passado quase seis meses sem que o erro fosse corrigido e, não havia motivo para pensar que alguma coisa fosse mudar. De fato, o inverno chegou e Wiles tinha esgotado inúmeras abordagens que poderiam ter reparado o erro e não enxergava mais nenhum caminho potencial para a solução. Até que admitiu para um amigo, Peter Sarnak, que a situação estava ficando desesperadora e que ele estava a ponto de aceitar a derrota. Sarnak sugeriu que parte da dificuldade poderia ser pelo fato de Wiles não ter ninguém em quem pudesse confiar no dia a dia, que pudesse avaliar suas ideias ou que o inspirasse a explorar abordagens paralelas do problema. Ele sugeriu que Wiles encontrasse alguém de confiança e que tentasse mais uma vez concertar a demonstração. Wiles pensou sobre o assunto e, então, decidiu convidar Richard Taylor, um professor de Cambridge, para ir trabalhar em Princeton com ele.

Taylor era um dos avaliadores da demonstração e um ex-aluno de Wiles. Além disso, era um matemático com muita experiência na teoria que envolvia o erro encontrado. No ano anterior ele estivera na plateia do Instituto Isaac Newton vendo seu supervisor apresentar a demonstração do século. Agora ele tentaria ajudar a resgatar essa demonstração.

Apesar de muito trabalho em conjunto, Wiles e Taylor passaram a primavera e o verão sem progressos. Depois de oito anos contínuos e a obsessão de uma vida inteira Wiles estava preparado para admitir a derrota. Ele disse a Taylor que não via motivos para continuar com suas tentativas para concertar a demonstração. No entanto, Taylor já havia planejado passar o mês de setembro em Princeton, antes de retornar a Cambridge e então, apesar do desânimo de Wiles, ele sugeriu que continuassem tentando por mais um mês. Se não houvesse progresso até final de setembro, eles desistiriam, reconhecendo publicamente o fracasso. A prova com o erro seria então publicada, para permitir que outros matemáticos tivessem a oportunidade de examiná-la.

Então, Wiles decidiu passar o mês de setembro examinando uma última vez o método envolvido no erro encontrado, para determinar, exatamente, por que ele não estava funcionando. E, subitamente, no dia 19 de setembro de 1994, quando estava examinando seu método, ele percebeu que, embora o método não estivesse funcionando completamente, ele era tudo o que Wiles precisava para construir uma abordagem correta para sua demonstração. Wiles não podia acreditar como deixou de perceber aquilo. Então, abordou sua nova ideia e, durante o dia, voltou

várias vezes em sua mesa para ver se a solução ainda estava lá. Era o momento mais importante de sua vida profissional.

Na manhã seguinte, ele já havia verificado inúmeras vezes sua demonstração e estava satisfeito. Então, contou à sua esposa: "Consegui! Acho que encontrei!". Mas foi tão inesperado que ela pensou que ele estivesse falando sobre um brinquedo de seus filhos, e ela respondeu: "Encontrou o quê?". E ele disse: "Eu consertei minha demonstração.". Assim, no mês seguinte Wiles pôde cumprir a promessa que não conseguira cumprir no ano anterior. Na noite de aniversário dela, ele lhe entregou o manuscrito completo.

Desta vez não havia dúvidas quanto à demonstração. Os dois trabalhos, de 130 páginas ao todo, eram os manuscritos matemáticos mais minuciosamente examinados em toda a história e foram publicados em maio de 1995 no *Annals of Mathematics*.

Para a demonstração do Último Teorema de Fermat, Wiles criou técnicas matemáticas completamente novas e as combinou com técnicas tradicionais de um modo que nunca fora considerado possível. E ao fazer isto ele criou novas linhas de ataque para todo um conjunto de outros problemas. De acordo com Ken Ribet, a prova é a síntese perfeita da matemática moderna e uma inspiração para o futuro. Assim, pode-se perceber que a demonstração é uma obra-prima da matemática moderna, o que leva à conclusão inevitável que a demonstração de Wiles para o Último Teorema de Fermat não é a mesma de Fermat.

E se Fermat não tinha a demonstração de Wiles, o que é que ele tinha? Os matemáticos se dividem em dois grupos. Os céticos acreditam que o Último Teorema de Fermat foi resultado de um momento de fraqueza do gênio do século XVII e que ele tinha somente uma demonstração equivocada. No entanto, matemáticos otimistas e românticos, acreditam que Fermat teria uma prova genuína.

O que quer que tenha sido, a prova de Fermat teria sido baseada na matemática do século XVII e teria um argumento tão astucioso que escapou a todos, de Euler a Wiles. Assim, apesar da publicação de Wiles para o problema, existem muitos matemáticos que acreditam que podem ficar famosos descobrindo a demonstração original de Fermat.

5.2 Dois casos particulares do Último Teorema de Fermat

Inicialmente apresentamos alguns conceitos e resultados sobre os triplos pitagóricos, importantes para o estudo dos casos particulares que são apresentados em seguida.

Definição 15. Uma terna de números naturais (x,y,z) chama-se triplo Pitagórico se satisfaz a equação $x^2+y^2=z^2$. O triplo (x,y,z) chama-se primitivo se $\text{mdc}(x,y,z)=1$.

Exemplo 28. As ternas $(4,3,5),(8,6,10),...,(4n,3n,5n),...$ e também $(12,5,13),(24,10,26),...,$ $(12n,5n,13n),...$ são triplos Pitagóricos sendo que $(4,3,5)$ e $(12,5,13)$ são primitivos.

Observação 12. Com qualquer triplo Pitagórico (x_1, y_1, z_1) primitivo e qualquer $n \in \mathbb{N}$, a terna (nx_1, ny_1, nz_1) também é um triplo Pitagórico, sendo que se $n > 1$ estes últimos não serão primitivos.

Diante disso, segue também o seguinte resultado.

Proposição 28. Seja (x, y, z) um tripo Pitagórico qualquer , d =mdc(x, y, z), e tome $x_1 = \frac{x}{d}$, $y_1 = \frac{y}{d}$, $z_1 = \frac{z}{d}$. Então (x_1, y_1, z_1) é um triplo Pitagórico primitivo e vale $(x, y, z) = (dx_1, dy_1, dz_1)$.

Demonstração. Considerando mdc$(x, y, z) = 1$ e tomando $x_1 = \frac{x}{1}$, $y_1 = \frac{y}{1}$ e $z_1 = \frac{z}{1}$ temos, de imediato que $(x, y, z) = (1 \cdot x_1, 1 \cdot y_1, 1 \cdot z_1)$ e com mdc$(x_1, y_1, z_1) =$ mdc$(x, y, z) = 1$, faz com que (x_1, y_1, z_1) seja um triplo Pitagórico primitivo.

Agora, considerando (x, y, z) um triplo Pitagórico qualquer e sendo d = mdc(x, y, z) temos $x_1 = \frac{x}{d}$,$y_1 = \frac{y}{d}$ e $z_1 = \frac{z}{d}$ com mdc$(x_1, y_1, z_1) = 1$, pois

$$\text{mdc}\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right) = \text{mdc}\left(\frac{x}{\alpha}, \text{mdc}\left(\frac{y}{\alpha}, \frac{z}{\alpha}\right)\right) = \text{mdc}\left(\frac{x}{\alpha}, 1\right) = 1.$$

Além disso, (x_1, y_1, z_1) é um triplo Pitagórico, pois de $x^2 + y^2 = z^2$ temos que:

$$x_1^2 + y_1^2 = \left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = \frac{x^2}{d^2} + \frac{y^2}{d^2} = \frac{x^2 + y^2}{d^2} = \frac{z^2}{d^2} = \left(\frac{z}{d}\right)^2 = z_1^2$$

Portanto, (x_1, y_1, z_1) é um triplo Pitagórico primitivo e $(x, y, z) = (dx_1, dy_1, dz_1)$. □

Da Proposição 28 vemos que para se classificar os triplos Pitagóricos, é suficiente a restrição aos primitivos.

Proposição 29. Seja (x, y, z) um triplo Pitagórico primitivo. Então exatamente um dos números x ou y é par, o outro é ímpar e z é ímpar.

Demonstração. Suponhamos x e y ambos pares, sendo $x = 2k$ e $y = 2l$, com $k, l \in \mathbb{Z}$. Como $z^2 = x^2 + y^2 = (2k)^2 + (2l)^2 = 4(k^2 + l^2)$, o que implica $z = 2t, t \in \mathbb{Z}$.Portanto, z seria par e mdc$(x, y, z) \geqslant 2$, o que nos traz um absurdo, já que mdc$(x, y, z) = 1$.

Agora, vamos supor x e y ambos ímpares, com $x = 2k + 1$ e $y = 2l + 1$, sendo $k, l \in \mathbb{Z}$. Assim, como $x^2 + y^2 = z^2$, temos que

$$z^2 = (2k+1)^2 + (2l+1)^2 = 4k^2 + 4k + 1 + 4l^2 + 4l + 1 = 4(k^2 + k + l^2 + l) + 2,$$

o que implica que $z^2 = 4t + 2, t \in \mathbb{Z}$, o que é impossível para um quadrado perfeito par, que pele Proposição 7 deve ser múltiplo de 4, na forma $4t', t \in \mathbb{Z}$.

Portanto exatamente um dos números x ou y é par, e z é ímpar. □

Deixaremos pré-estabelecido que quando (x,y,z) é um triplo Pitagórico, x é par e y é ímpar.

Proposição 30. Seja (x,y,z) um triplo Pitagórico primitivo. Então

$$\text{mdc}(x,y) = \text{mdc}(y,z) = \text{mdc}(x,z) = 1,$$

isto é, x,y,z são primos entre si, tomados dois a dois.

Demonstração. Se $\text{mdc}(x,y) = d$, sendo $d > 1$ então existe um divisor primo p de d tal que $p|x$ e $p|y$. Dessa forma $p|x^2$ e $p|y^2$ e então $p|x^2+y^2 = z^2$. Portanto, pela Proposição 17, $p|z$ e então $\text{mdc}(x,y,z) \geqslant p$. O que é um absurdo, já que mdc(x,y,z)=1.

Para os outros dois casos temos a mesma demonstração. □

Proposição 31. Sejam $n,m,c \in \mathbb{N}$ com $n.m = c^2$ e $\text{mdc}(m,n) = 1$. Então existem $N,M \in \mathbb{N}$ tais que $n = N^2$ e $m = M^2$, isto é, n e m são quadrados perfeitos individualmente.

Demonstração. Sejam $n = \prod_{k=1}^{r} p_k^{a_k}$ e $m = \prod_{k=1}^{s} q_k^{b_k}$ as decomposições primárias de n e m. Sabemos que pelo fato de $\text{mdc}(m,n) = 1$, q_k são diferentes do p_l.

Segue que $n \cdot m = p_1^{a_1} \cdot \ldots \cdot p_r^{a_r} \cdot q_1^{b_1} \cdot \ldots \cdot q_s^{b_s}$ é a decomposição primária de $n \cdot m$. Como $n \cdot m = c^2$ e c^2 é quadrado perfeito, temos que todos os $a_1, \ldots, a_r, b_1, \ldots, b_s$ são pares.

Portanto, temos $n = N^2$ e $m = M^2$ sendo $N = \prod_{k=1}^{r} p_k^{\frac{a_k}{2}}$ e $M = \prod_{k=1}^{s} q_k^{\frac{b_k}{2}}$. □

Agora estamos em condições de provar o teorema de classificação dos triplos Pitagóricos dado a seguir.

Teorema 16. a) Escolhendo-se números $s,t \in \mathbb{N}$ com $s > t \geqslant 1$, $\text{mdc}(s,t) = 1$, $s-t$ ímpar e tomando-se $x = 2st$, $y = s^2 - t^2$ e
$z = s^2 + t^2$, temos que (x,y,z) será um triplo Pitagórico primitivo.

b) Qualquer triplo Pitagórico primitivo é obtido pelo método no item a).

Demonstração. a) Iniciaremos a demonstração mostrando que $x = 2st$, $y = s^2 - t^2$ e $z = s^2 + t^2$ é um triplo Pitagórico. De fato, temos que

$$x^2 + y^2 = (2st)^2 + (s^2 - t^2)^2 = 4s^2t^2 + s^4 - 2s^2t^2 + t^4 = s^4 + 2s^2t^2 + t^4 = (s^2 + t^2)^2 = z^2.$$

Seguiremos mostrando que o triplo Pitagórico é primitivo e para isso vamos supor que ele não seja e chegaremos num absurdo. Supondo $p|\text{mdc}(x,y,z)$ para algum primo p. Então p é ímpar e de $p|x$ temos $p|2st$, o que implica que $p|s$ ou $p|t$. Como $p|z$ e $z = s^2 + t^2$ temos que $p|s$ e $p|t$, o que é um absurdo, neste caso $p \leqslant \text{mdc}(s,t) = 1$.

b) Seja (x,y,z) um triplo Pitagórico qualquer. com x par, y ímpar e z ímpar. Sabemos que $z^2 = x^2 + y^2$. Logo, $x^2 = z^2 - y^2 = (z+y)(z-y)$ e, como $z+y$ e $z-y$ são pares segue que $\frac{x^2}{4} = \frac{(z+y)}{2} \cdot \frac{z-y}{2} \in \mathbb{N}$. Ou seja,

$$\left(\frac{x}{2}\right)^2 = n \cdot m$$

com $n = \frac{z+y}{2}$ e $m = \frac{z-y}{2}$. Além disso, se $d = \text{mdc}(n,m)$, então $d|n \pm m$ mas $n+m = \frac{z+y}{2} + \frac{z-y}{2} = z$ e $n-m = \frac{z+y}{2} - \frac{z-y}{2} = y$ e, assim $d|\text{mdc}(y,z)$. Mas como (x,y,z), sabemos pela Proposição 30 que $\text{mdc}(y,z) = 1$. Logo, $d = 1$, o seja. $\text{mdc}(n,m) = 1$.

Assim, como $\left(\frac{x}{2}\right)^2 = n \cdot m$ e $\text{mdc}(n,m) = 1$, segue pela Proposição 31 que n e m são quadrados perfeitos. ou seja, $n = s^2$ e $m = t^2$ com $s,t \in \mathbb{N}$. Logo, $\text{mdc}(s,t) = \text{mdc}(n,m) = 1$ e $s-t$ é ímpar. Além disso, notamos que $s^2 - t^2 = n - m = y$, $s^2 + t^2 = n + m = z$ e de $\left(\frac{x}{2}\right)^2 = n \cdot m = s^2 t^2$, concluímos que $x = 2st$.

□

Observação 13. Do Teorema 16 pode-se notar que existem infinitos triplos Pitagóricos primitivos. por exemplo, podemos iniciar uma sequência tomando (s,t) como pares $(2,1),(3,2),(4,1),(4,3),(5,2),(5,4),(6,1),(6,5)$, etc.

Observação 14. Os triplos Pitagóricos, primitivos e não-primitivos, são obtidos por

$$(2nst, n(s^2-t^2), n(s^2+t^2))$$

em que $n,s,t \in \mathbb{N}$ com $s > t \geqslant 1$, $\text{mdc}(s,t) = 1$, $s-t$ ímpar.

Note que em qualquer triplo Pitagórico primitivo (x,y,z), x é múltiplo de 4 e y é ímpar e maior que 1.

Os triplos Pitagóricos primitivos são numerosos, como mostra a seguinte proposição.

Proposição 32. a) Qualquer número ímpar maior que 1 é o y de pelo menos um triplo Pitagórico primitivo.

b) Todo número natural divisível por 4 é o x de pelo menos um triplo Pitagórico primitivo.

Demonstração. a) Se y é ímpar, temos $y = 2k-1, k \in \mathbb{N}, k > 1$ e pelo Teorema 16, temos $y = s^2 - t^2$, sendo y maior que 1.

Daí, de $s^2 - t^2 = 2k-1$, segue que $(s+t)(s-t) = 2k-1$ e uma solução para isso seria $s+t = 2k-1$ e $s-t = 1$, ou seja, $s = k$ e $t = k-1$.

Dessa forma, como $x = 2st$ e $z = s^2 + t^2$, temos o seguinte triplo pitagórico com y dado

$$(2k(k-1); 2k-1, k^2 + (k-1)^2).$$

b) Se x é divisível por 4 temos $x = 4k$, $k \in \mathbb{N}$ e pelo Teorema 16, $x = 2st$ e uma solução para isso seria $s = 2k$ e $t = 1$ e assim, com $y = s^2 - t^2$ e $z = s^2 + t^2$, temos o seguinte número pitagórico com x dado

$$(4k, 4k^2 - 1, 4k^2 + 1).$$

□

Note que para $y > 1$ ímpar obtemos tantos triplos primitivos $(.,y,.)$ quantas decomposições multiplicativas $y = kl$ com $\text{mdc}(k,l) = 1$ existirem. Podemos associar tal fato à consequência 24 estudada anteriormente.

Note que y é ímpar e $y = k \cdot l$ então $\text{mdc}(k,l) = 1$. De fato se y é ímpar, k e l também são ímpares. Dessa forma, seja $d = \text{mdc}(k,l)$, temos certamente $d \neq 2$. Agora, pela Proposição 24, se $y = s^2 - t^2$ então $y = \left(\frac{k+l}{2}\right)^2 - \left(\frac{k-l}{2}\right)^2$, sendo $s = \frac{k+l}{2}$ e $t = \frac{k-l}{2}$.

Suponha que $\text{mdc}(k,l) = d \neq 1$, então $d|k$ e $d|l$. Logo, existem $k_1, l_1 \in \mathbb{Z}$ tal que $k = k_1 \cdot d$ e $l = l_1 \cdot d$,

$$\text{mdc}(s,t) = \text{mdc}\left(\frac{k+l}{2}, \frac{k-l}{2}\right) = \text{mdc}\left(\frac{k_1 \cdot + l_1 d}{2}, \frac{k_1 d - l_1 d}{2}\right) = d \cdot \text{mdc}\left(\frac{k_1 + l_1}{2}, \frac{k_1 - l_1}{2}\right) \neq 1,$$

o que é contradição, já que pelo Teorema 16 $\text{mdc}(s,t) = 1$.

Exemplo 29. Para qualquer primo $p > 2$, o único triplo pitagórico da forma $(.,p,.)$ é $\left(\frac{p^2-1}{2}, p, \frac{p^2+1}{2}\right)$. E este é necessariamente primitivo.

Exemplo 30. a) Para qualquer primo $p > 2$ dado, os triplos Pitagóricos da forma $(.,p^2,.)$ são:

i um único não-primitivo $p.\left(\frac{p^2-1}{2}, p, \frac{p^2+1}{2}\right)$;

ii um único primitivo $\left(\frac{p^4-1}{2}, p^2, \frac{p^4+1}{2}\right)$.

b) Em geral para qualquer primo $p > 2$ e $n \in \mathbb{N}$ dados, os triplos Pitagóricos da forma $(.,p^n,.)$ são:

i um único primitivo $\left(\frac{p^{2n}-1}{2}, p^n, \frac{p^{2n}+1}{2}\right)$;

ii $n-1$ não primitivos $p^{n-k}\left(\frac{p^{2k}-1}{2}, p^k, \frac{p^{2k}+1}{2}\right)$, sendo $k \in \{1,2,...,n-1\}$.

Exemplo 31. Para quaisquer dois primitivos $2 < q < p$, os triplos da forma $(.,pq,.)$ são:

i dois não-primitivos $p.\left(\frac{q^2-1}{2}, q, \frac{q^2+1}{2}\right)$ e q.$\left(\frac{p^2-1}{2}, p, \frac{p^2+1}{2}\right)$;

ii dois primitivos $\left(\frac{p^2q^2-1}{2}, pq, \frac{p^2q^2+1}{2}\right)$ e $\left(\frac{p^2-q^2}{2}, pq, \frac{p^2+q^2}{2}\right)$.

5.2.1 O caso $n = 4$

Nesta seção mostraremos, na verdade, o caso $4|n$ e, portanto, o caso $n = 4$ do Último Teorema de Fermat.

Proposição 33. Sejam $n, a, b, c \in \mathbb{N}$ tais que $a|n, b|n, c|n$. Se existem números $x, y, z \in \mathbb{N}$ tais que $x^n + y^n = z^n$, então existem também x', y' e $z' \in \mathbb{N}$ tais que $x'^a + b'^b = z'^c$.

Demonstração. Se $a|n, b|n, c|n$ então existem $r, s, t \in \mathbb{N}$ tais que $n = a.r, n = b.s$ e $n = c.t$. Daí, se $x^n + y^n = z^n$ temos $x^{ar} + y^{bs} = z^{ct}$ e então $(x^r)^a + (y^s)^b = (z^t)^c$. Fazendo $x^r = x'$, $y^s = y'$ e $z^t = z'$ temos $x'^a + y'^b = z'^c$. □

Observação 15. Seja $n \in \mathbb{N}$. Da Proposição acima vemos que se existirem números $a, b, c \in \mathbb{N}$ com $a|n$, $b|n$, $c|n$ tais que $x^a + y^b = z^c$ é impossível para $x, y, z \in \mathbb{N}$ é impossível $x^n + y^n = z^n$ com $x, y, z \in \mathbb{N}$.

Esta observação reduz o problema do Teorema de Fermat para um tratamento somente com expoentes primos. Ou seja, por que $x^p + y^p = z^p$ é impossível para todos os primos $p > 2$?

Observação 16. Seja $n \in \mathbb{N}$ com $4|n$. Como consequência da discussão acima se $x^4 + y^4 = z^2$ é impossível para $x, y, z \in \mathbb{N}$, então também $x^n + y^n = z^n$ é impossível com $x, y, z \in \mathbb{N}$.

O Teorema abaixo garante a demonstração do teorema de Fermat quando $4|n$.

Teorema 17. A equação $x^4 + y^4 = z^2$ não possui uma solução $x, y, z \in \mathbb{N}$.

Demonstração. Vamos considerar o conjunto $\mathbb{S} = \{z \in \mathbb{N} | \exists x, y \in \mathbb{N} \text{ com } x^4 + y^4 = z^2\}$.

Supondo que a equação $x^4 + y^4 = z^2$ tenha solução com $x, y, z \in \mathbb{N}$, teríamos $\mathbb{S} \neq \emptyset$.

Sendo $\mathbb{S}$ um subconjunto dos Números Naturais, temos $z_0 \in \mathbb{S}$ sendo z_0 o elemento mínimo. de S Dessa forma, existem x_0, y_0 pertencentes $\mathbb{N}$ com $z_0^2 = x_0^4 + y_0^4$.

A partir daí, tomando $z_1 < z_0, z_1 \in \mathbb{N}$, então não existem $x_1, y_1 \in \mathbb{N}$ com $z_1^2 = x_1^4 + y_1^4$. Assim, nossa demonstração consiste em construirmos, a partir de (x_0, y_0, z_0) um triplo $x_1, y_1, z_1 \in \mathbb{N}$ com $z_1^2 = x_1^4 + y_1^4$, sendo $z_1 < z_0$. Ao obter tal resultado, chegaremos numa contradição.

Primeiramente demonstraremos que o $\text{mdc}(x_0, y_0) = 1$.

Admitindo $d = \text{mdc}(x_0, y_0)$, chamaremos $\frac{x_0}{d}$ e $\frac{y_0}{d}$, respectivamente, de x_1 e y_1.

Daí, temos que

$$x_1^4 + y_1^4 = \left(\frac{x_0}{d}\right)^4 + \left(\frac{y_0}{d}\right)^4 = \frac{x_0^4 + y_0^4}{d^4} = \frac{z_0^2}{d^4} = \left(\frac{z_0}{d^2}\right)^2 = z_1^2, \text{ onde } z_1 = \frac{z_0}{d^2}.$$

Se $d > 1$, temos $z_0 > z_1$, o que é absurdo, já que z_0 é o elemento mínimo de S. Portanto, $d = \text{mdc}(x_0, y_0) = 1$.

De $\text{mdc}(x_0, y_0) = 1$ temos $\text{mdc}(x_0^2, y_0^2) = 1$. Ao assumir a existência de $x_0, y_0 \in \mathbb{N}$ com $x_0^4 + y_0^4 = z_0^2$, temos a equação equivalente $(x_0^2)^2 + (y_0^2)^2 = z_0^2$ e daí temos (x_0^2, y_0^2, z_0) um triplo Pitagórico primitivo, já que $\text{mdc}(x_0^2, y_0^2, z_0) = \text{mdc}(\text{mdc}(x_0^2, y_0^2)), z_0) = \text{mdc}(1, z_0) = 1$.

Pelo Teorema 16 existem $s, t \in \mathbb{N}$ com $s > t$, $\text{mdc}(s,t) = 1$ e $s - t$ ímpar tal que $x_0^2 = 2st$, $y_0^2 = s^2 - t^2$ e $z_0 = s^2 + t^2$. Como $s - t$ é ímpar temos duas possibilidades: s par e t ímpar ou s ímpar e t par. Percebemos facilmente que a segunda é a verdadeira. De fato, se s fosse par, teríamos $s = 2s'$ e $t = 2t' + 1$ com $s', t' \in \mathbb{N}$ e então

$$y_0^2 = (2s')^2 - (2t' + 1)^2 = 4s'^2 - 4t'^s - 4t' - 1 = 4(s'^2 - t'^2 - t') - 1 = 4l - 1,$$

com $l \in \mathbb{N}$. O que é impossível para um quadrado perfeito. Pois como vimos na Proposição 7, um quadrado perfeito ímpar deveria ter a forma $4k + 1, k \in \mathbb{N}$.

Logo, dado que t é par e s é ímpar, tomaremos $t = 2r$ com $r \in \mathbb{N}$ e obteremos $x_0^2 = 2st = 2s \cdot 2r = 4sr$ e daí, temos: $\frac{x_0^2}{4} = rs$, ou seja, $\left(\frac{x_0}{2}\right)^2 = rs$.

Como $\text{mdc}(s,t) = 1$, temos $\text{mdc}(s, 2r) = 1$ com $\text{mdc}(s, 2) = 1$ e então $\text{mdc}(s, r) = 1$. A partir daí e da relação $\left(\frac{x_0}{2}\right)^2 = r.s$, temos que r e s são quadrados perfeitos, pela Proposição 31. Digamos então que $s = z_1^2$ e $r = w_1^2$, com $z_1, w_1 \in \mathbb{N}$.

De $y_0^2 = s^2 - t^2$ temos $y_0^2 + t^2 = s^2$. Como $\text{mdc}(s,t) = 1$, temos que $\text{mdc}(t, y_0, s)$=$\text{mdc}(1, y_0)$ e então (t, y_0, s) é um triplo Pitagórico primitivo. Logo, existem $u, v \in \mathbb{N}$ com $u > v$, $u - v$ ímpar, $\text{mdc}(u, v) = 1$, tais que t=2uv, $y_0 = u^2 - v^2$ e $s = u^2 + v^2$.

De $t = 2uv$ temos que $\frac{t}{2} = uv$ e como $t = 2r$, então $r = uv$ e de $w_1^2 = r$, temos $w_1^2 = uv$. Mais uma vez, da Proposição 31 temos que u e v são individualmente quadrados perfeitos e os chamaremos, respectivamente de x_1^2 e y_1^2, com $x_1, y_1 \in \mathbb{N}$. Logo, $x_1^4 + y_1^4 = u^2 + v^2 = s = z_1^2$,o que mostra que z_1 é um elemento do conjunto $\mathbb{S}$.

Como $0 < z_1 < z_1^2$ temos $0 < z_1 < s$, já que $z_1^2 = s$, e de $s < s^2$ temos que $0 < z_1 < s^2 < s^2 + t^2 = z_0$. Ou seja, $0 < z_1 < z_0$, e chegamos num absurdo, já que z_0 é elemento mínimo de $\mathbb{S}$.

Portanto, $\mathbb{S}$ é vazio e dessa forma, $x^4 + y^4 = z^2$ não pode ser solúvel em $\mathbb{N}$. □

5.2.2 O caso n=3

A seguir faremos a demonstração do teorema de Fermat para o caso $n = 3$. Para isso apresentamos inicialmente o seguinte resultado.

Lema 2. Se s é ímpar e $s^3 = a^2 + 3b^2$ com $\text{mdc}(a, b) = 1$ então s também será da forma $s = u^2 + 3v^2$com $u, v \in \mathbb{Z}$ e

$$\begin{cases} a = u(u^2 - 9v^2) \\ b = 3v(u^2 - v^2) \end{cases}$$

Demonstração. Para a prova que s também pode ser escrito com $s = u^2 + 3v^2$ referimos (RIBENBOIM, 2000) Lema 4.7.

Para a demonstração da segunda parte do lema serão usados argumentos já trabalhados anteriormente, em conexão com o estudo de inteiros da forma $u^2 + 3v^2$. Seja S o conjunto de todos os inteiros da forma $(a^2 + 3b^2)$, com $a, b \in \mathbb{Z}$. S é claramente fechado para a multiplicação, pois

$$\begin{aligned}(a^2+3b^2)(c^2+3d^2) &= a^2c^2+3a^2d^2+3b^2c^2+9b^2d^2 \\ &= a^2c^2+3a^2d^2+3b^2c^2+9b^2d^2+6abcd-6abcd \\ &= (a^2c^2 \pm 6abcd+9b^2d^2)+3(a^2d^2 \mp 2abdc+b^2c^2) \\ &= (ac \pm 3bd)^2+3(ad \pm bc)^2\end{aligned} \tag{5.1}$$

onde a igualdade está assegurada com os sinais correspondentes.

Agora, tomando $s \in S$, com $s = u^2 + 3v^2$, com $u, v \in \mathbb{Z}$, temos que

$$\begin{aligned}s^2 = (u^2+3v^2)^2 = u^4+6u^2v^2+9v^4 &= u^4+6u^2v^2+9v^4+6u^2v^2-6u^2v^2 \\ u^4-6u^2v^2+9v^4+12u^2v^2 &= (u^2-3v^2)^2+3(2uv)^2,\end{aligned}$$

o que mostra que $s^2 \in S$. Usando a igualdade obtida acima concluímos ainda que

$$s^3 = (u^2+3v^2)^3 = (u^2+3v^2)^2.(u^2+3v^2) = [(u^2-3v^2)^2+3(2uv)^2](u^2+3v^2).$$

Podemos associar a última expressão com o que foi obtido em 5.1 e concluímos que

$$(u^2+3v^2)\cdot(u^2-3v^2)^2+3(2uv)^2] = (u\cdot[u^2-3v^2]) - 3v[2uv])^2+3(u\cdot[2uv]+v[u^2-3v^2])^2.$$

Logo,

$$\begin{aligned}s^3 &= (u^3-3uv^2-6uv^2)^2+3(2u^2v+u^2v-3v^3)^2 \\ &= (u^3-9uv^2)^2+3(3u^2v-3v^3)^2 = (u[u^2-9v^2])^2+3(3v[u^2-v^2])^2 = a^2+3b^2.\end{aligned}$$

Ou seja, $s^3 = a^2 + 3b^2$ com

$$\begin{cases} a = u(u^2-9v^2) \\ b = 3v(u^2-v^2) \end{cases}$$

□

Observação 17. Na demonstração do Teorema abaixo também usaremos algumas vezes a seguinte propriedade do mdc: $\text{mdc}(ac, b) = 1 \iff \text{mdc}(a, b) = \text{mdc}(c, b) = 1$.

Teorema 18. Não existe uma solução de inteiros não nulos para a equação $x^3 + y^3 + z^3 = 0$.

Demonstração. Assuma que $x,y,z \in \mathbb{Z}$, $z,y,z \neq 0$, com $\text{mdc}(x,y) = \text{mdc}(x,z) = \text{mdc}(y,z) = 1$ são tais que $x^3+y^3+z^3 = 0$. Então x, yez são distintos, pois se dois deles fossem iguais teríamos por exemplo $x^3+y^3+y^3 = 0$, ou seja, $x^2 = -2y^3$ e como 2 não é um cubo perfeito, chegamos num absurdo.

Além disso, sabemos que exatamente um desses inteiros é par. De fato, se os três fossem ímpares teríamos que a soma de dois ímpares resultaria num número ímpar, que também é absurdo. Se os três fossem pares eles não seriam primos entre si(dois a dois). Ainda, se fossem dois pares e um ímpar teríamos a soma de dois pares sendo um número ímpar. Portanto a única configuração possível é a de dois números ímpares e um par. Digamos x e y ímpares e z par.

Entre todas as possíveis soluções com as propriedades acima escolhemos uma para o qual $|z|$ é a menor escolha possível, ou seja $|z|$ é o mínimo de $S = \{z \in \mathbb{N}/\exists x,y \text{ com } x^3+y^3+z^3 = 0\}$ e x,y,z primos entre si.

Vamos encontrar inteirosp,m,n primos entre si, dois a dois, satisfazendo a equação $p^3+m^3n^3 = 0$, onde n é par e $|z| > |n|$. Isto irá gerar uma contradição, pois teríamos uma sequência infinita decrescente de inteiros positivos.

Visto que x e y são ímpares $(x+y)$ e $(x-y)$ são pares, então existem inteiros a e b tais que $(x+y) = 2a$ e $(x-y) = 2b$ e então $x = a+b$ e $y = a-b$, sendo a e b não nulos com $\text{mdc}(a,b) = 1$ e paridades distintas.

Segue da equação $x^3+y^3+z^3 = 0$ que $x^3+y^3 = -z^3$. E com $x = a+b$ e $y = a-b$, temos

$$-z^3 = (a+b)^3+(a-b)^3 = a^3+3a^2b+3ab^2+b^3+a^3-3a^2b+3ab^2-b^3 = 2a(a^2+3b^2).$$

Como a e b tem paridades distintas, (a^2+3b^2) é ímpar. Como definido anteriormente, z é par e dessa forma $8|z^3$ e $8|2a$. De fato, temos que

$$8|z^3 \Rightarrow 8|2a(a^2+3b^2) \Rightarrow 8|2a,$$

já que como a^2+3b^2 é ímpar, $8 \nmid a^2+3b^2$.

Agora, de $8|2a$ temos que a é par e portanto b é ímpar. Com a par e b ímpar vamos verificar que $\text{mdc}(2a,a^2+3b^2) = 1$ ou $\text{mdc}(2a,a^2+3b^2) = 3$.

De fato, seja q um número primo e q^k um fator comum de $2a$ e a^2+3b^2. Então $2a = q^k.c$ e $(a^2+3b^2) = q^k.d$, se c e $d \in \mathbb{Z}$.

Como (a^2+3b^2) é ímpar, temos $q \neq 2$ e ainda $q^k|a$, já que $q^k|2a$ e $q \nmid 2$. Logo, temos que $q^k|(a^2+3b^2)$ e $q^k|a^2$, o que implica que $q^k|3b^2$.

Como $\text{mdc}(a,b) = 1$ e $q|a$ temos que $q \nmid b$ e então $q^k \nmid b^2$. Portanto $q^k|3$ e assim $k = 1$ e $q = 3$.

Agora, consideremos então cada um dos casos citados acima.

Caso 1: $\text{mdc}(2a,a^2+3b^2) = 1$.

Note que 3 não divide a caso contrário dividiria também $2a$ e a^2+3b^2 e então o $\text{mdc}(2a, a^2+3b^2) \geqslant 3$, o que não satisfaz nossa condição. Da equação $-z^3 = 2a(a^2+3b^2)$ e considerando que para esse caso $2a$ e a^2+3b^2 são primos entre si, segue da fatoração única de inteiros em primos que $2a$ e a^2+3b^2 são cubos perfeitos. Assim,

$$\begin{cases} 2a = r^3, \\ a^2+3b^2 = s^3 \end{cases}$$

em que s é ímpar, já que a é par e b é ímpar. Além disso, s não é múltiplo de 3, já que a não é múltiplo de 3. Logo temos que s é ímpar e $s^3 = a^2+3b^2$ com $\text{mdc}(a,b) = 1$, então pelo Lema 2 s também será da forma $s = u^2+3v^2$, com $u, v \in \mathbb{Z}$ e ainda:

$$\begin{cases} a = u(u^2-9v^2) \\ b = 3v(u^2-v^2) \end{cases}$$

Assim, como b é ímpar, temos v ímpar e u par. Sabendo que 3 não divide a sabemos que 3 não divide $u(u^2-9v^2)$ e então 3 não divide u e u é não nulo.

Com $\text{mdc}(u,v) = 1$, temos $2u, u+3v$ e $u-3v$ primos entre si, dois a dois. De fato, é claro que $\text{mdc}(u+3v, u-3v) = 1$. Além disso como $\text{mdc}(u,u,\pm 3v) = \text{mdc}(u,3v) = \text{mdc}(u,v) = 1$ e $\text{mdc}(2, u\pm 3v) = 1$, então $\text{mdc}(2u, u\pm 3v) = 1$.

De início, temos $r^3 = 2a$ e daí

$$r^3 = 2a = 2u(u^2-9v^2) = 2u(u+3v)(u-3v).$$

Com o mesmo argumento usado anteriormente, se $2u(u+3v)(u-3v)$ é um cubo perfeito, então $2u, u+3v$ e $u-3v$ também serão cubos perfeitos. Então,

$$\begin{cases} 2u = -n^3 \\ u-3v = p^3 \\ u+3v = m^3 \end{cases}$$

Sobre p, m e n, concluímos que são não nulos já que $3 \nmid u$ e primos entre si dois a dois.

Além disso, temos que $p^3+m^3+n^3 = u-3v+u+3v-2u = 0$. E mais,

$$|z^3| = |2a\cdot(a^2+3b^2)| = |2u(u^2-9v^2)\cdot(a^2+3b^2)|.$$

Como $(u^2-9v^2) = (u+3v)\cdot(u-3v) = p^3\cdot m^3 \neq 0$ e a^2+3b^2 com b ímpar é maior ou igual a 3, temos que

$$|z|^3 = |2u(u^2-9v^2)\cdot(a^2+3b^2)| \geqslant |-n^3|\cdot|p^3\cdot m^3|\cdot 3 > |n^3|.$$

Portanto, $|z|^3 > |n|^3 \Rightarrow |z| > |n|$.

Disso, temos que a terna (p,m,n) é a solução da equação $X^3+Y^3+Z^3=0$ com $|z|>|n|$, o que contradiz o fato de $|z|$ ser mínimo.

Caso 2: mdc$(2a,a^2+3b^2)=3$

Note que neste caso, $3|2a$ e então $3|a$ e que faz com que a seja da forma $a=3c$, $c\in\mathbb{Z}$. Além disso, como $8|2a$ temos que $4|a$ e então $4|3c$ o que implica que $4|c$ e portanto, c é par. Como mdc$(a,b)=1$ e $3|a$, então $3\nmid b$.

Da equação $-z^3=2a(a^2+3b^2)=2(3c)(9c^2+3b^2)=18c(3c^2+b^2)$.

Afirmamos que mdc$(18c,3c^2+b^2)=1$. De fato, já que c é par e b é ímpar, temos que $3c^2+b^2$ ímpar, $3\nmid 3c^2+b^2$, pois $3\nmid b$ e mdc$(b,c)=1$.

Ainda de $-z^3=18c(3c^2+b^2)$ e pela fatoração única de inteiros temos que $18c$ e $3c^2+b^2$ são cubos perfeitos. Assim,

$$\begin{cases} 18c=r^3, \\ 3c^2+b^2=s^3 \end{cases}$$

em que s é ímpar e $3|r$. Logo, temos que s é ímpar e $s^3=(b^2+3c^2)$ com mdc(b,c)=1 então pelo Lema 2 s também será da forma $s=(u^2+3v^2)$, com $u,v\in\mathbb{Z}$ e

$$\begin{cases} b=u(u^2-9v^2) \\ c=3v(u^2-v^2) \end{cases}$$

Deste modo, temos que u é ímpar, v é par, já que b é ímpar, v não nulo e mdc$(u,v)=1$.

Logo, $2v$, $(u+v)$ e $(u-v)$ são relativamente primos entre si, dois a dois. De fato, como mdc$(v,u)=1\Rightarrow$mdc$(v,u\pm v)=1$, e mdc$(2,u\pm v)$=1, temos que mdc$(2v,u\pm v)=1$. E mais, de mdc$(v,u)=1$ segue que mdc$(u+v,u-v)=1$.

Do início temos $r^3=18c=18.[3v(u^2-v^2)]=54v(u+v)(u-v)$. Logo,

$$\left(\frac{r}{3}\right)^3=2v(u+v)(u-v).$$

Assim, $2v,u+veu-v$ são cubos perfeitos:

$$\begin{cases} 2v=-n^3 \\ u+v=p^3 \\ u-v=-m^3 \end{cases}$$

Além disso, na terna (p,m,n) todos são diferentes de 0, relativamente primos entre si e satisfazem a equação $x^3+y^3+z^3=0$, pois

$$p^3+m^3+n^3=(u+v)+(-u+v)-2v=0$$

finalmente notando que

$$\begin{aligned} |z|^3 &= |18c \cdot (3c^2 + b^2)| \\ &= |9 \cdot 2 \cdot 3v(u^2 - v^2)\ cdot(3c^2 + b^2)| \\ &= 27 \cdot |2v \cdot (u^2 - v^2)| \cdot |3c^2 + b^2| \\ &= 3^3 \cdot |n|^3 \cdot |u^2 - v^2| \cdot |3c^2 + b^2| \\ &= 3^3 |n^3| |-p^3 m^3| |3c^2 + b^2| > |n^3| \end{aligned}$$

Daí $|z|^3 > |n|^3$ e assim $|z| > |n|$

Ou seja, temos que a terna (p,m,n) é solução da equação $X^3 + Y^3 + Z^3 = 0$ com $|z| > |n|$, o que contradiz o fato de $|z|$ ser mínimo. □

REFERÊNCIAS

BRUNO, S. da S. **O último teorema de Fermat para n=3**. Monografia (Mestrado Profissional em Matemática em Rede Nacional) — Universidade Federal do Estado do Rio de Janeiro, 2014. Citado na página 16.

HEFEZ, A. **Aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática, 1^a edição, 2013. Citado na página 16.

MAIER, R. R. **Teoria dos números - Texto de aula**. [S.l.]: Universidade de Brasília. Departamento de Matemática, 2005. Citado na página 16.

RIBENBOIM, P. **Fermat's last theorem for amateurs**. New York: Springer Verlag, 2000. Citado na página 85.

SINGH, S. **O último Teorema de Fermat**. Rio de Janeiro, São Paulo: Editora Record, 2011. Citado na página 16.


ICMC
USP
SÃO CARLOS