

Teorema Fundamental da Aritmética

Luciene Parron Gimenes - DMA - UEM

Um conceito fundamental em aritmética é a ideia de números primos. Do ponto de vista da estrutura multiplicativa dos inteiros são os mais simples e ao mesmo tempo são suficientes para gerar todos os inteiros como veremos adiante no Teorema Fundamental da Aritmética. Também veremos a definição de congruência e alguns critérios de divisibilidade. Tendo conhecimento destes resultados, mostramos como a prova dos nove funciona e também veremos uma dinâmica interessante chamada de O Nove Misterioso.

Sumário

1	Alguns conceitos e resultados	1
2	Números primos	4
3	Teorema Fundamental da Aritmética	6
4	Congruência e Divisibilidade	7
5	Prova dos nove	8
6	Divisibilidade	10
7	O Nove Misterioso	11
8	Exercícios	12
9	Agradecimentos	13

1 Alguns conceitos e resultados

Antes de apresentarmos o Teorema Fundamental da Aritmética, vamos introduzir alguns conceitos e enunciar resultados que serão necessários para nosso entedimento.

O primeiro resultado nos diz que todo subconjunto de $\mathbb{Z}$ limitado inferiormente possui mínimo.

Teorema 1.1 (Princípio do menor inteiro) *Se $S \subset \mathbb{Z}$, $S \neq \emptyset$ e S é limitado inferiormente, então existe $l_0 \in S$ tal que $l_0 \leq x$, para todo $x \in S$.*

A seguir, enunciamos dois princípios de indução úteis para provarmos vários resultados na matemática.

Teorema 1.2 (Primeiro princípio de indução) *Suponhamos que sejam dados um inteiro a e uma afirmação $P(n)$ dependendo de $n \in \mathbb{Z}$, $n \geq a$ e que podemos provar as seguintes propriedades:*

- (i) $P(a)$ é verdadeira;
- (ii) para cada inteiro $k \geq a$, se $P(k)$ for verdadeira, então $P(k+1)$ também é verdadeira.

Então, $P(n)$ é verdadeira, para todo inteiro $n \geq a$.

Teorema 1.3 (Segundo princípio de indução) *Suponhamos que sejam dados um inteiro a e uma afirmação $P(n)$ dependendo de $n \in \mathbb{Z}$, $n \geq a$ e que podemos provar as seguintes propriedades:*

- (i) $P(a)$ é verdadeira;
- (ii) dado um inteiro $l > a$, se $P(k)$ for verdadeira, para todo $a \leq k < l$, então $P(l)$ também é verdadeira.

Então, $P(n)$ é verdadeira, para todo inteiro $n \geq a$.

Agora apresentamos o algoritmo da divisão que garante que dados dois inteiros, a divisão de um deles pelo outro (não nulo) é sempre possível, mesmo que para isso tenhamos que deixar um resto.

Teorema 1.4 (Algoritmo de Euclides) *Dados dois inteiros a e b , $b > 0$, existe um único par de inteiros q e r , com $0 \leq r < b$, tais que*

$$a = qb + r.$$

Observemos que embora no enunciado do Teorema 1.4 exista a restrição $b > 0$, isto se faz necessário. É possível enunciar o Algoritmo da divisão da seguinte forma: Dados dois inteiros a e b , $b \neq 0$, existe um único par de inteiros q e r tais que $a = qb + r$ com $0 \leq r < |b|$.

Definição 1.5 Seja $a, b \in \mathbb{Z}$. Dizemos que b é um múltiplo de a ou, então, que a divide b se existir um inteiro k tal que $b = ka$. Notação: $a|b$ (lê-se a divide b).

Exemplo 1.6 6 é múltiplo de 3 ou $3|6$, pois $6 = 2 \times 3$.

Teorema 1.7 (Propriedades da divisão) Sejam $a, b \in \mathbb{Z}$.

- (i) $a|a$, para todo $a \in \mathbb{Z}$, $a \neq 0$.
- (ii) Se $a|b$ e $b|a$, então $a = b$, $a, b \in \mathbb{Z}_+$.
- (iii) Se $a|b$ e $b|c$, então $a|c$.
- (iv) Se $a|b$ e $a|c$, então $a|bx + cy$, para todo $x, y \in \mathbb{Z}$.

Exemplo 1.8 Como $3|15$ e $3|42$, então $3|(8 \times 15 - 7 \times 42)$.

Definição 1.9 O máximo divisor comum de dois inteiros a e b (a ou b diferente de zero), denotado por $\text{mdc}(a, b)$, é o maior inteiro que divide a e b .

Teorema 1.10 Quaisquer que sejam $a, b \in \mathbb{Z}$ com $a > 0$ e $b > 0$, existe o máximo divisor comum entre a e b .

Demonstração: Sejam $S = \{ax + by; x, y \in \mathbb{Z}\}$ e $S' = \{s \in S; s > 0\}$. Notemos que $S' \neq \emptyset$, pois $a + b > 0$ e $a + b = a \cdot 1 + b \cdot 1 \in S$.

Como S' é limitado inferiormente, pelo Princípio do Menor Inteiro, existe $d \in S'$ tal que $d \leq x$, para todo $x \in S'$. Vamos mostrar que $d = \text{mdc}(a, b)$, ou seja, devemos verificar que

- (i) $d \geq 0$, pois $d \in S'$.
- (ii) $d|a$ e $d|b$.

Como $a, d \in \mathbb{N}$ e $d > 0$, pelo Algoritmo da Divisão, existem $q, r \in \mathbb{N}$ com $0 \leq r < d$ tais que

$$a = qd + r. \quad (11)$$

Vamos mostrar que $r = 0$.

Como $d \in S' \subset S$, existem $x_0, y_0 \in \mathbb{Z}$ tais que

$$d = ax_0 + by_0. \quad (12)$$

Substituindo (12) em (11), obtemos

$$a = qd + r = q(ax_0 + by_0) + r.$$

Daí, $r = a(1 - qx_0) + b(-q)y_0$. Logo, $r \in S$. Como $0 \leq r < d$, devemos ter $r = 0$. Assim, de (11), segue que $a = qd$, ou seja, $d|a$.

Analogamente, mostramos que $d|b$.

(iii) Se $d'|a$ e $d'|b$, então $d'|d$.

Se $d'|a$ e $d'|b$, então de (12), segue que $d'|d$.

Como (i)-(iii) estão satisfeitas, concluímos que $d = \text{mdc}(a, b)$, como queríamos demonstrar. $\square$

Corolário 1.11 *Seja d o máximo divisor comum de a e b , então existem inteiros x_0 e y_0 tais que $d = x_0a + y_0b$.*

Na demonstração do Teorema 1.10 mostramos, não apenas que o máximo divisor comum de a e b pode ser expresso como uma combinação destes números, mas que este número é o menor valor positivo dentre todas estas combinações lineares.

2 Números primos

Nesta seção, vamos conhecer algumas propriedades elementares de números primos.

Definição 2.1 *Um número inteiro $p \geq 2$ é primo se os seus divisores positivos são somente 1 e p .*

Exemplo 2.2 *2, 3, 5, 7, 11, 13, 17 são números primos.*

Teorema 2.3 (Euclides) *A sequência dos números primos é infinita.*

Demonstração: Vamos supor que a sequência dos números primos seja finita. Seja $p_1, p_2, \dots, p_n$ a lista de todos os primos. Consideremos o número

$$N = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1.$$

Sabemos que todo número maior do que 1 ou é primo ou é composto (escrito como produto de números primos). O N definido acima não é divisível por

nenhum dos p_i , $1 \leq p_i \leq n$ e é maior do que p_i , assim tal divisão teria resto 1. Logo, N é maior do que todos os primos conhecidos e esse número N ou é primo ou é composto. Se N for primo descobrimos um número que não estava na sequência dada e portanto a sequência de números primos não é finita. Se N for composto, então ele é produto de primos, e como vimos esses fatores primos não podem ser nenhum dos números da sequência original, novamente achamos mais um número primo que não estava na sequência original, provando a infinidade dos primos. $\square$

Proposição 2.4 *Todo número inteiro $a \geq 2$ possui pelo menos um divisor primo.*

Demonstração: Fixado $a \in \mathbb{Z}$, ≥ 2 , defina

$$S = \{x \in \mathbb{Z}; x \geq 2, x|a\}.$$

Temos que $S \neq \emptyset$, pois $a|a$ e $-a|a$ e $a \geq 2$.

Queremos provar que o mínimo de S é um número primo. É claro que S é limitado inferiormente. Pelo Princípio do Menor Inteiro, Teorema 1.1, existe $p \in S$ tal que $p \leq x$, para todo $x \in S$.

Suponhamos que p não seja primo. Então, existe $q \in \mathbb{Z}$, $q \neq 1$, $q \neq \pm p$ tal que $q|p$. Temos, então $2 \leq |q| < p$ e $|q|$ divide a , pois $|q||p|$ e $p|a$. Logo, $|q| \in S$. Absurdo! Portanto, p é primo. $\square$

Proposição 2.5 *Se p é um número primo e $p|ab$, onde $a, b \in \mathbb{Z}$, então $p|a$ ou $p|b$.*

Demonstração: Suponha que p não divida a . Como p é primo e p não divide a , os únicos inteiros que dividem p e a são 1 e -1 . Então, $\text{mdc}(a, p) = 1$. Logo, pelo Teorema 1.10, existem $x_0, y_0 \in \mathbb{Z}$ tais que

$$1 = px_0 + ay_0. \quad (23)$$

Multiplicando ambos os lados de (23) por b , obtemos

$$b = p(x_0b) + (ab)y_0. \quad (24)$$

Como $p|p$ e $p|ab$, segue de (24) que $p|b$. $\square$

Corolário 2.6 *Se p é um primo e $p|a_1.a_2 \dots a_n$, então $p|a_i$, para algum $1 \leq i \leq n$.*

3 Teorema Fundamental da Aritmética

A seguir, apresentamos um dos principais teoremas da aritmética que diz que todo número inteiro maior ou igual a 2 pode ser escrito como produto de números primos. Por exemplo, 2100 é escrito de maneira única, a menos pela ordem dos fatores, como $2^2 \times 3^1 \times 5^2 \times 7^1$.

A ordem dos fatores, pela propriedade comutativa da multiplicação, é irrelevante. O que torna tal teorema interessante é a garantia de obtenção de uma representação única para todo e qualquer número natural. Isso abre diversas possibilidades de aplicação, como em criptografia, onde um texto pode ser codificado como uma sequência de números primos.

Teorema 3.1 (Teorema Fundamental da Aritmética) *Todo inteiro $a \geq 2$ pode ser escrito como produto de números primos. Esta decomposição é única exceto pela ordem dos fatores primos.*

Demonstração: Usaremos o Segundo princípio de indução sobre $a \geq 2$. Vamos denotar por $P(a)$ a afirmação: “ a se escreve de modo único como produto de primos exceto pela ordem dos fatores”. É claro que $P(2)$ é verdadeira. Suponhamos que $P(k)$ seja verdadeira, para todo $2 \leq k < a$. Como $a > 2$, pelo Lema 2.4, existe um número primo p_1 tal que $p_1|a$, ou seja, existe $q \in \mathbb{Z}$ tal que $a = p_1 q$. Se $q = 1$ ou q é primo, então $P(k)$ é verdadeira, caso contrário, $2 \leq q < a$. Pela hipótese de indução, existem $p_2, \dots, p_r$ primos maiores que zero tais que

$$q = p_2 \dots p_r.$$

Assim, $a = p_1 \cdot q = p_1 \cdot p_2 \dots p_r$, provando que a pode ser escrito como r produto de primos. Resta provar a unicidade.

Suponhamos que

$$a = p_1 \cdot p_2 \dots p_r \quad \text{e} \quad a = q_1 \cdot q_2 \dots q_s, \quad (35)$$

com p_i, q_j primos maiores que 0 e $1 \leq i \leq r, 1 \leq j \leq s$. Como $p_1|q_1 \cdot q_2 \dots q_s$, então $p_1|q_i$, para algum $i, 1 \leq i \leq s$, sem perda de generalidade, podemos supor $i = 1$. Daí, $p_1|q_1$ e como q_1 é primo, devemos ter $p_1 = q_1$.

De (35), temos

$$p_1 \cdot p_2 \dots p_r = p_1 \cdot q_2 \dots q_s.$$

Como $p_1 \neq 0$, simplificando, obtemos $p_2 \dots p_r = q_2 \dots q_s$. Repetindo este processo, chegaremos que $r = s$ e após um rearranjo dos índices q_j , encontramos $p_1 = q_1, p_2 = q_2, \dots, p_r = q_r$. $\square$

4 Congruência e Divisibilidade

Seja $m \in \mathbb{Z}$, $m \neq 0$. Dizemos que os inteiros a e b são congruentes módulo m se os restos das divisões de a e b por m são iguais. Neste caso, escrevemos

$$a \equiv b \pmod{m}.$$

Observamos que, quando $m = 1$, quaisquer dois inteiros são sempre congruentes módulo 1; além disso, se $a \equiv b \pmod{m}$, então $a \equiv b \pmod{-m}$. Logo, podemos supor $m \geq 2$.

É fácil verificar que $a \equiv b \pmod{m}$ se, e somente se, m divide $(a - b)$. De fato, se $a \equiv b \pmod{m}$, então $a = mq + r$ e $b = mq' + r$, onde $0 \leq r < m$. Logo, $a - b = m(q - q')$ e, assim $m | (a - b)$. Reciprocamente, se $m | (a - b)$, pela divisão euclidiana, podemos escrever $a = mq + r$ e $b = mq' + r'$, onde $0 \leq r, r' < m$. Logo, $(a - b) = m(q - q') + (r - r')$. Como $m | (a - b)$ e $m | m(q - q')$, então $m | (r - r')$. Segue que $r = r'$, pois $0 \leq |r - r'| < m$. Portanto, $a \equiv b \pmod{m}$. Por exemplo, $3 \equiv 1 \pmod{2}$, pois $2 | (3 - 1)$.

Sejam a, b, c, d, m, n inteiros, $m > 1$ e $n \geq 1$. As seguintes propriedades valem:

- (a) $a \equiv a \pmod{m}$.
- (b) Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.
- (c) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.
- (d) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $(a + c) \equiv (b + d) \pmod{m}$.
- (e) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ac \equiv bd \pmod{m}$.
- (f) Se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$.

As propriedades (a), (b) e (c) dizem que a relação de congruência em $\mathbb{Z}$ é uma relação de equivalência em $\mathbb{Z}$. Como uma relação de equivalência dá uma partição para o conjunto, segue que a relação de congruência módulo m divide $\mathbb{Z}$ em classes de equivalência as quais são chamadas de classes residuais ou classes dos restos das divisões por m .

Seja $a \in \mathbb{Z}$. Denotamos por $\bar{a}$ a classe de equivalência do inteiro a , isto é,

$$\bar{a} = \{x \in \mathbb{Z}; x \equiv a \pmod{m}\}.$$

No conjunto das classes de restos das divisões por m , representado por $\mathbb{Z}_m$, podemos definir as seguintes operações:

$$\bar{a} + \bar{b} = \overline{a + b} \quad (\text{adição}) \quad \text{e} \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b} \quad (\text{multiplicação}).$$

Afirmamos que $(\mathbb{Z}_m, +)$ é um grupo abeliano. Antes de verificarmos os axiomas de grupo precisamos provar que a operação $+$ está bem definida. Como ela opera com classes, devemos provar que $\bar{a} + \bar{b}$ não depende dos representantes a e b das classes $\bar{a}$ e $\bar{b}$. Sejam a, a' elementos da classe $\bar{a}$ e b, b' elementos da classe $\bar{b}$, segue que $(a - a') = mq$ e $(b - b') = mp$. Logo, $(a + b) - (a' + b') = m(q + p)$, isto é, $(a + b) - (a' + b') = m(q + p)$. Ou seja, $(a + b) \equiv (a' + b') \pmod{m}$ e, assim, $\overline{a + b} = \overline{a' + b'}$. A verificação dos axiomas de grupo é deixado como exercício.

A operação multiplicação em $\mathbb{Z}_m$ também está bem definida, pois se $\bar{a} = \bar{a'}$ e se $\bar{b} = \bar{b'}$, então $a \equiv a' \pmod{m}$ e $b \equiv b' \pmod{m}$ e, assim, $m|(a - a')$ e $m|(b - b')$. Como

$$a.b - a'.b' = a(b - b') + b'(a - a'),$$

então segue que $m|(a.b - a'.b')$, isto é, $(a.b) \equiv (a'.b') \pmod{m}$.

5 Prova dos nove

Nas séries iniciais do ensino básico, quando o professor ensina adição e multiplicação, ele também ensina a prova dos nove. Este é um teste para verificar se a conta está correta. Vamos relembrar este teste? O teste consiste em somar os dígitos das parcelas e realizar a operação com a soma dos dígitos, se o resultado da operação com a soma dos dígitos for diferente da soma dos dígitos do resultado da conta, então a operação realizada está incorreta.

Consideremos o produto $4436 \times 291 = 1290876$. A soma dos algarismos na primeira parcela é 17 o que resulta em 8 e na segunda parcela a soma é 12 o que resulta em 3; portanto, $8 \times 3 = 24$ que resulta em 6. No resultado, a soma dos seus algarismos é 33, o que resulta em 6.

Quando olhamos para a soma dos algarismos, estamos olhando para o resto da divisão por 9: como $4436 = 492 \times 9 + 8$ e $291 = 32 \times 9 + 3$, temos que os restos 8 e 3, resultando em 24, dando portanto 6. Enquanto que $1290876 = 143430 \times 9 + 6$ tem resto 6.

Qual a explicação para o funcionamento deste teste? A explicação está na divisão por 9.

Primeiramos, observemos que

$$\begin{aligned} 10 &= 9 + 1 \\ 100 &= 99 + 1 \\ 1000 &= 999 + 1 \\ &\vdots \\ 10^n &= \underbrace{9999 \cdots 9}_n + 1 \end{aligned}$$

Segue que $10^n = 1 + 9q$, para algum $q \in \mathbb{Z}$. Multiplicando 10^n por qualquer a , obtemos

$$a10^n = a + 9aq.$$

Consideremos M e N inteiros. Podemos escrevê-los da forma

$$\begin{aligned} M &= a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10^1 + a_0 10^0 \\ N &= b_n 10^n + b_{n-1} 10^{n-1} + \cdots + b_1 10^1 + b_0 10^0. \end{aligned}$$

Por exemplo, $291 = 2 \times 10^2 + 9 \times 10^1 + 1 \times 10^0$ e $4436 = 4 \times 10^3 + 4 \times 10^2 + 3 \times 10^1 + 6 \times 10^0$.

Lembrando que $a10^n = a + 9aq$, ficamos com

$$\begin{aligned} M &= (a_m + 9a_m q_m) + (a_{m-1} + 9a_{m-1} q_{m-1}) + \cdots + (a_1 + 9a_1 q_1) + (a_0 + 9a_0 q_0) \\ N &= (b_n + 9b_n q_n) + (b_{n-1} + 9b_{n-1} q_{n-1}) + \cdots + (b_1 + 9b_1 q_1) + (b_0 + 9b_0 q_0). \end{aligned}$$

Considerando a soma $M + N$, obtemos que

$$M + N = (a_m + \cdots + a_1 + a_0 + b_n + \cdots + b_1 + b_0) + 9s,$$

para algum inteiro s . Assim, a soma dos algarismos das parcelas M e N quando dividida por 9 deixa o mesmo resto que $M + N$ quando divididos por 9.

De modo análogo, o produto

$$M \times N = (a_m + \cdots + a_1 + a_0) \times (b_n + \cdots + b_1 + b_0) + 9t,$$

para algum inteiro t . Novamente, o produto das somas dos dígitos das parcelas M e N quando dividido por 9, deixa o mesmo resto que $M \times N$.

Isto explica o funcionamento do teste chamado de **prova dos noves**. Convém chamar a atenção para o seguinte: o teste diz apenas quando a sua conta está errada, isto é, se os resultados forem diferentes a conta está errada. Este teste não nos diz em hipótese alguma se a conta está correta.

6 Divisibilidade

Com as ideias usadas no entendimento da prova dos nove, podemos obter alguns critérios de divisibilidade.

Teorema 6.1 (Critério de divisibilidade por 9) *9 divide a se, e somente se, 9 divide a soma dos algarismos de a .*

Demonstração: Dado qualquer $n \geq 1$, tem-se $10^n = 1 + 9q$, para algum inteiro q , segue que $10^n - 1 = 9q$, ou seja, $9|(10^n - 1)$ e, portanto, $10^n \equiv 1 \pmod{9}$. Então, $a_n 10^n \equiv a_n \pmod{9}$, para todo $n \geq 1$.

Logo,

$$\begin{aligned} a &= a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10^1 + a_0 \\ &\equiv (a_n + a_{n-1} + \dots + a_1 + a_0) \pmod{9}. \end{aligned}$$

Portanto, 9 divide a se, e somente se, 9 divide a soma dos algarismos de a . $\square$

Como 9 divide $10^n - 1$, então 3 também divide $10^n - 1$, e assim, o corolário seguinte é imediato e sua prova segue do teorema acima.

Corolário 6.2 (Critério de divisibilidade por 3) *3 divide a se, e somente se, 3 divide a soma dos algarismos de a .*

Exemplo 6.3 *4578 não é divisível por 9, pois $(4 + 5 + 7 + 8) = 24$ não é divisível por 9.*

Exemplo 6.4 *4578 é divisível por 3, pois $(4 + 5 + 7 + 8) = 24$ é divisível por 3.*

Teorema 6.5 (Critério de divisibilidade por 2) *2 divide a se, e somente se, a termina em 0, 2, 4, 6 ou 8.*

Demonstração: Temos que

$$a - a_0 = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10^1.$$

Como $10^n \equiv 0 \pmod{2}$, temos $a \equiv a_0 \pmod{2}$. Portanto, 2 divide a se, e somente se, a_0 é par. $\square$

Teorema 6.6 (Critério de divisibilidade por 5) *5 divide a se, e somente se, a termina em 0 ou 5.*

Demonstração: Como

$$a - a_0 = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10^1$$

e $10^n \equiv 0 \pmod{5}$, temos $a \equiv a_0 \pmod{5}$. Portanto, 5 divide a se, e somente se, a_0 é 0 ou 5. $\square$

7 O Nove Misterioso

Usando indução e propriedades dos números naturais, vamos desvendar a solução do jogo chamado de O Nove Misterioso. Veja [1].

Dado um número inteiro N , se fizermos uma permutação de seus algarismos, obteremos um outro inteiro N' . Se alguém omitir um algarismo, que não seja o zero, da diferença $N - N'$ e revelar quais são os demais algarismos desta diferença conseguiremos sempre adivinhar qual foi o algarismo omitido.

Vamos desvendar este mistério?

Definição 7.1 *Uma permutação sobre um conjunto $A \neq \emptyset$ é uma bijeção de σ em A .*

Dado um inteiro $N = a_n a_{n-1} \dots a_1 a_0$, em notação decimal,

$$N = a_n 10^n + \dots + a_1 10^1 + a_0 10^0.$$

Assim, de uma permutação dos algarismos de N , resulta um inteiro N' que, em notação decimal, se escreve como

$$N' = a_n 10^{\sigma(n)} + \dots + a_1 10^{\sigma(1)} + a_0 10^{\sigma(0)}.$$

Lema 7.2 *9 divide $(10^n - 1)$, para todo $n \in \mathbb{N}$.*

Demonstração: A demonstração pode ser feita por indução. Observe que $(10^n - 1)$ é um número constituído apenas de noves. $\square$

Lema 7.3 *9 divide $(10^n - 10^m)$, quaisquer que sejam $m, n \in \mathbb{N}$.*

Demonstração: Para ver isto, basta observar, pelo lema anterior, que $9|(10^n - 1)$ e $9|(10^m - 1)$, quaisquer que sejam os naturais m e n . Portanto, 9 divide a diferença, isto é, $9|(10^n - 10^m)$. $\square$

Finalmente, temos o seguinte resultado que desvenda o mistério.

Teorema 7.4 9 divide $(N - N')$, onde N e N' são dados acima.

Demonstração: Observemos que

$$N - N' = a_n(10^n - 10^{\sigma(n)}) + \dots + a_1(10^1 - 10^{\sigma(1)}) + a_0(10^0 - 10^{\sigma(0)}).$$

Como $9|(10^n - 10^m)$ para quaisquer naturais m e n , segue que $9|(10^r - 10^{\sigma(r)})$ e, portanto, $9|(N - N')$. E o teorema está provado. $\square$

Está desvendado, assim, o mistério do **nove misterioso**. De fato, se $N - N'$ é sempre divisível por 9, o algarismo omitido da diferença é aquele que somado aos demais dá um número divisível por 9.

8 Exercícios

1. Seja a um inteiro. Mostre que se a é par, então a^2 também é par. Mostre que se a é ímpar, então a^2 também é ímpar.
2. Mostre que se a é inteiro e a^2 é par, então a é par.
3. Seja $a \geq 2$ par. Mostre que a^2 deve ser decomposto em uma quantidade par de números primos.
4. Mostre que, para todo inteiro positivo t , $\text{mdc}(ta, tb) = t \text{mdc}(a, b)$.
5. Mostre que se $\text{mdc}(a, b) = d$, então $\text{mdc}(\frac{a}{d}, \frac{b}{d}) = 1$.
6. Mostre que $\sqrt{2}$ é irracional.

Solução: Suponhamos, por absurdo, que $\sqrt{2}$ seja um número racional. Então, $\sqrt{2} = \frac{a}{b}$, com $a, b \in \mathbb{Z}$ e $b \neq 0$. Sem perda de generalidade, supomos que $\text{mdc}(a, b) = 1$.

Notemos que

$$2 = \frac{a^2}{b^2} \Rightarrow a^2 = 2b^2 \Rightarrow a^2 \text{ é par.}$$

Logo, a é um número par, ou seja, $a = 2k$, para algum $k \in \mathbb{Z}$.

Como $\sqrt{2} = \frac{a}{b}$, segue que

$$2 = \frac{a}{b} = \frac{(2k)^2}{b^2} \Rightarrow 2b^2 = 4k^2 \Rightarrow b^2 = 2k^2 \Rightarrow b^2 \text{ é par.}$$

Logo, b também é um número par, ou seja, $b = 2k'$, para algum $k' \in \mathbb{Z}$. Portanto, o máximo divisor comum entre a e b deve ser maior ou igual a 2, o que é uma contradição. $\square$

7. Mostre que $\sqrt{2.3.5}$ é irracional.

Solução: Seja $\sqrt{2.3.5} = \frac{a}{b}$, com $a, b \in \mathbb{Z}$ e $b \neq 0$. Então, elevando ambos os lados ao quadrado, obtemos $2.3.5 = \frac{a^2}{b^2}$. Então,

$$2.3.5.b^2 = a^2.$$

Sabemos que a^2 possui uma quantidade par de números primos. Por outro lado, temos $2.3.5.b^2$, o que possui uma quantidade ímpar de números primos. Uma contradição, pois a decomposição é única, exceto pela ordem dos fatores primos. $\square$

8. Um macaco sobe uma escada de dois em dois degraus e sobra um degrau, sobe de 3 em 3 degraus e sobram 2. Quantos degraus tem a escada sabendo que o número de degraus é múltiplo de 7 e está compreendido entre 40 e 100.

9 Agradecimentos

Agradeço especialmente ao prof. Doherty Andrade pelas várias sugestões e pela utilização do seu material nesse texto. Agradeço também aos internautas por outras correções.

Referências

- [1] D. Andrade, *O nove misterioso*, RPM no. 09 (1985). 7
- [2] José Plínio de Oliveira Santos, *Introdução a teoria dos números*, Coleção Matemática Universitária 3 ed. Rio de Janeiro, IMPA, 2009.
- [3] D. Andrade, *Curso de Introdução à Álgebra: notas de aula*, UEM (1992).