UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL - PROFMAT

(Mestrado)

SUZANA PAULA MARTOS

A PROVA DOS NOVES E ESTIMATIVAS DE ERROS

Maringá-PR

2018

SUZANA PAULA MARTOS

A PROVA DOS NOVES E ESTIMATIVAS DE ERROS

Trabalho de Conclusão de Curso apresentado ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre.
Área de concentração: Matemática.

Orientador: Prof. Dr. Rodrigo Martins

Maringá

2018

Dados Internacionais de Catalogação-na-Publicação (CIP)

M35j

Martos, Suzana Paula.
A prova dos noves e estimativas de erros / Suzana Paula Martos. -- Maringá (PR), 2018.
57 f.

Orientador: Prof. Dr. Rodrigo Martins.
Dissertação (mestrado) – Universidade Estadual de Maringá, Centro de Ciências Exatas, Departamento Matemática. Programa de Mestrado Profissional em Matemática, 2018.

1. Divisibilidade. 2. Congruências. 3. Falha da prova dos noves. I. Martins, Rodrigo, orient. II. Universidade Estadual de Maringá, Centro de Ciências exatas, Departamento de Matemática. Programa de Mestrado Profissional em Matemática. III. Título.

CDD 510

Rosângela A. A. Silva – CRB 9ª/1810

SUZANA PAULA MARTOS

A PROVA DOS NOVES E ESTIMATIVAS DE ERROS

Trabalho de Conclusão de Curso, apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática tendo a Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:

Prof. Dr. Rodrigo Martins
DMA/Universidade Estadual de Maringá (Orientador)

Prof. Dr. Jamil Viana Pereira
Universidade Estadual Paulista "Júlio de Mesquita Filho" – Rio Claro

Profa. Dra. Luciene Parron Gimenes Arantes
DMA/Universidade Estadual de Maringá

Aprovada em: 06 de abril de 2018.
Local de defesa: Auditório do DMA, Bloco F67, campus da Universidade Estadual de Maringá.

Agradecimentos

Ao concluir este trabalho, agradeço:

À CAPES, pelo fundamental apoio financeiro.

Ao meu orientador, Prof. Dr. Rodrigo Martins, pela orientação, paciência, incentivo e valiosas considerações que tornaram possível a conclusão deste trabalho.

À minha família, minha irmã Karina Martos e aos meus pais, Paulo A. Martos e Cleuza S. Martos pelo apoio e incentivo.

À todos meus amigos que estiveram comigo durante esta jornada, que deram força e compartilharam inúmeras e inesquecíveis horas de estudos, de risadas e preocupações.

À todos que, direta ou indiretamente, contribuíram para a realização deste trabalho.

Resumo

Neste trabalho apresentamos um estudo sobre números inteiros, divisibilidade, sistemas de numeração e congruência, que fundamentam o tema deste trabalho, que é a prova dos noves. A prova dos noves é um método de verificação de operações matemáticas básicas com números naturais, mas que caiu em desuso atualmente. Mostraremos como se aplica a prova dos noves, em quais resultados matemáticos ela se baseia, quando e porquê a prova dos noves pode falhar. Por fim, apresentaremos estimativas de falhas da prova dos noves.

Palavras-chave: Divisibilidade, Congruências, Falha da Prova dos Noves.

Abstract

In this work we present a study about integers numbers, divisibility, numbering systems and congruence, that bases the work theme, “The Proof by Nine”. The Proof by Nine is a method of verifying basic mathematical operations with natural numbers, but has fallen into disuse actually. We will show how this method is applied, in which mathematical results it is based, when and why it can fail. Finally, we will present estimates of failure of the proof by nine method.

Keywords: Divisibility, Congruences, Failure of the Proof by Nine.

Lista de Tabelas

Sumário

Introdução

A prova dos noves é uma regra que possibilita verificar se uma operação aritmética foi realizada corretamente.

Não foram encontradas referências que apontam a origem da prova dos noves e nem a partir de que época esta foi inserida nos currículos escolares. O que se encontram são indícios de que esta regra é um conceito de séculos passados, como aponta a bibliografia [5], que afirma que a prova dos noves já era mencionada na primeira aritmética árabe que se conhece, a de al-Khowârizmî, que viveu no século IX. Atualmente, a prova dos noves caiu em desuso e não é mais ensinada nas escolas, apesar de sua relevância para o cálculo mental e desenvolvimento cognitivo.

Assim, um dos objetivos desse trabalho é resgatar os conceitos da regra dos "noves fora", o que é a prova dos noves e como ela funciona, por meio de demonstrações de resultados que são as bases dessa prova. Para isso, nos capítulos iniciais foi necessário fazer uma revisão bibliográfica sobre números inteiros, divisibilidade, sistemas de numeração e congruência.

Outro fato, que nos motivou ao estudo da prova dos noves, é que a mesma é uma condição necessária, mas não suficiente, e que ela pode falhar. Em outras palavras, se determinada operação matemática for realizada corretamente, certamente a prova dos noves vai indicar que a operação está correta. Entretanto, se a operação aritmética não for realizada corretamente, a prova dos noves nem sempre identificará o erro. Essa questão nos chamou a atenção e nos motivou a fazer um estudo sobre o porquê da prova dos noves poder falhar e quando ela falha.

Além disso, apresentaremos casos particulares da porcentagem de falha da prova dos noves, isto é, qual a probabilidade da prova dos noves não identificar o erro em uma determinada operação matemática, já que não encontramos na bibliografia pesquisada essa abordagem, nem relatos sobre a porcentagem de falhas da prova dos noves.

Capítulo 1

Os números inteiros

Ao falar da prova dos noves, é importante apresentar uma visão algébrica dos números inteiros. Por isso, neste capítulo apresentaremos as propriedades elementares do conjunto do números inteiros, o Princípio da Boa Ordenação e o Príncipio de Indução Finita. Para isto, usaremos como base a bibliografia [8].

Neste trabalho, denotaremos por $\mathbb{Z}$ o conjunto dos números inteiros e por $\mathbb{N}$, o conjunto dos números naturais.

1.1 Propriedades elementares

Em $\mathbb{Z}$, estão definidas as operações de soma e produto, de números inteiros:

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} & \qquad \cdot : \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z} \\ (x, y) &\longrightarrow x + y & (x, y) &\longrightarrow x \cdot y \end{aligned}$$

para todos $x, y, z \in \mathbb{Z}$, satisfazendo as seguintes propriedades:

1. $(x + y) + z = x + (y + z)$ (associatividade da soma)
2. Existe $0 \in \mathbb{Z}$ tal que $x + 0 = 0 + x = x$ (existência do elemento neutro)
3. Existe $-x \in \mathbb{Z}$ tal que $x + (-x) = (-x) + x = 0$ (existência do inverso aditivo de cada elemento $x \in \mathbb{Z}$)
4. $x + y = y + x$ (comutatividade da soma)
5. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (associatividade do produto)

6. Existe $1 \in \mathbb{Z}$ tal que $x \cdot 1 = 1 \cdot x = x$ (existência da unidade em $\mathbb{Z}$)

7. $x \cdot y = y \cdot x$ (comutatividade do produto)

8. $x \cdot (y + z) = x \cdot y + x \cdot z$ (distributividade do produto em relação à soma)

9. $x \cdot y = 0 \Rightarrow x = 0$ ou $y = 0$ ($\mathbb{Z}$ não possui divisores de zero)

Nestas condições, o conjunto $(\mathbb{Z}, +, \cdot)$ tem estrutura de anel comutativo, porém como em $\mathbb{Z}$ não existe inverso multiplicativo, ele não forma um corpo. Estas estruturas não serão abordadas neste texto, pois nosso enfoque é outro, mas para mais informações, veja [8].

1.2 Boa ordenação e o Princípio de indução finita

O objetivo desta seção é enunciar o Princípio da Boa Ordenação em $\mathbb{Z}$ e o Princípio da Indução Finita para a posterior demonstração de resultados importantes referente ao tema deste trabalho.

Proposição 1.1 (Princípio da boa ordenação.). *Todo subconjunto não vazio S de $\mathbb{Z}$ de elementos não negativos possui um primeiro elemento, isto é, existe $x_0 \in S$ tal que $x_0 \leq x$, para todo $x \in S$.*

Admitiremos o Princípio da Boa Ordenação como postulado com a finalidade de demonstrarmos o Princípio de Indução Finita. A seguir, enunciaremos uma proposição também importante para a demonstração do Princípio de Indução.

Proposição 1.2. *Não existe um número inteiro m tal que $0 < m < 1$.*

Demonstração. Suponhamos, por contradição, que existe $m \in \mathbb{Z}$ tal que $0 < m < 1$. Logo, o conjunto $S = \{m \in \mathbb{Z}; 0 < m < 1\}$ é não vazio e pelo Princípio da Boa Ordenação, S possui um menor elemento, isto é, existe $x_0 \in S$ tal que $x_0 \leq x$, para todo $x \in S$, e ainda, $0 < x_0 < 1$, pois $x_0 \in S$.

Como $x_0 \in S$, temos que $0 < x_0 < 1$ então $0 < x_0^2 < x_0 < 1$. Logo, $x_0^2 \in S$ e $x_0^2 < x_0$, o que é uma contradição, pois x_0 é o menor elemento de S.

■

Proposição 1.3 (Primeiro Princípio de Indução)**.** *Suponhamos que sejam dados um inteiro a e uma afirmação $P(n)$ dependendo de $n \in \mathbb{Z}$, $n \neq a$ 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 $n \geq a$.

Demonstração. Suponhamos que exista um conjunto S, não vazio, de inteiros m maiores que ou iguais a a tais que $P(m)$ seja falsa. Assim, pelo Princípio da Boa Ordenação, S possui um menor elemento, isto é, $x_0 \leq m$, $\forall m \in S$. Como $P(a)$ é verdadeira, por hipótese, temos que $a \notin S$ e portanto $x_0 > a$.

Disso, temos também que $(x_0 - 1) \notin S$ e portanto, $P(x_0 - 1)$ é verdadeira.

Agora, como $P(x_0 - 1)$ é verdadeira, temos pela hipótese (*ii.*) que $P[(x_0 - 1) + 1] = P(x_0)$ é verdadeira, o que é uma contradição, pois por hipótese assumimos que $x_0 \in S$ e $P(x_0)$ é falsa, concluindo a demonstração.

■

Proposição 1.4 (Segundo Princípio de Indução)**.** *Suponhamos que sejam dados um inteiro a e uma afirmação $P(n)$ dependendo de $n \in \mathbb{Z}$, $n \neq a$ 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 $n \geq a$.

Demonstração. Suponhamos que exista um conjunto S, não vazio, de inteiros m maiores que ou iguais a a tais que $P(m)$ seja falsa. Assim, pelo Princípio da Boa Ordenação, S possui um menor elemento x_0, isto é, existe $x_0 \in S$ tal que $x_0 \leq m$, $\forall m \in S$. E, como por hipótese $(i.)$, $P(a)$ é verdadeira, concluímos que $x_0 > a$.

Logo, $P(k)$ é verdadeira $\forall k$, com $a \leq k < x_0$ mas por $(ii.)$, $P(x_0)$ também é verdadeira, o que contradiz o fato de $x_0 \in S$, concluindo a demonstração.

■

Exemplo 1.5. Prove que $2 + 6 + 18 + \ldots + 2 \cdot 3^{n-1} = 3^n - 1$.

Devemos mostrar que

$$P(n) = 2 + 6 + 18 + \ldots + 2 \cdot 3^{n-1} = 3^n - 1,$$

é verdadeira, para todo $n \in \mathbb{N}$.

$(i.)$ $P(1)$ é verdadeira, pois $P(1) = 2 = 3^1 - 1$.

$(ii.)$ Suponhamos que $P(k)$ é verdadeira, para algum $k \in \mathbb{N}$, ou seja,

$$P(k) = 2 + 6 + 18 + \ldots + 2 \cdot 3^{k-1} = 3^k - 1 \text{ (HI)}.$$

Queremos mostrar que $P(k+1)$ é verdadeira. Notemos que,

$P(k+1) = \underbrace{2 + 6 + 18 + \ldots + 2 \cdot 3^{k-1}}_{(HI)} + 2 \cdot 3^{(k+1)-1}$

$P(k+1) = 3^k - 1 + 2 \cdot 3^k$

$P(k+1) = 3^k \cdot (1+2) - 1$

$P(k+1) = 3^k \cdot 3 - 1$

$P(k+1) = 3^{k+1} - 1.$

A última igualdade nos mostra que $P(k+1)$ é verdadeira. Logo, pelo Princípio de indução finita, $P(n)$ é verdadeira, para todo $n \in \mathbb{N}$.

■

Exemplo 1.6. Prove que $n^2 \geq 2n + 3$, para $n \geq 3$, $n \in \mathbb{N}$.

Devemos mostrar que $P(n) = n^2 \geq 2n + 3$, para $n \geq 3$.

$(i.)$ $P(3)$ é verdadeira, pois

$P(3) = 3^2 = 9 \geq 2 \cdot 3 + 3$.

$(ii.)$ Suponhamos $P(k)$ é verdadeira para algum $k \in \mathbb{N}$, $k \geq 3$, ou seja, $P(k) = k^2 \geq 2k+3$, para $n \geq 3$ (HI).

Queremos mostrar que $P(k+1)$ é verdadeira. Notemos que,

$P(k+1) = (k+1)^2 = k^2 + 2k + 1 \geq \underbrace{2k+3}_{(HI)} + 2k + 1 \geq 2k + 2 + 3 = 2(k+1) + 3$, pois $k \geq 3$.

Pelo Princípio de Indução Finita, $P(n)$ é verdadeira, para todo $n \in \mathbb{N}$.

$\blacksquare$

Capítulo 2

Divisibilidade

Neste capítulo, apresentaremos vários resultados referentes à divisibilidade de números inteiros. Inicialmente, apresentaremos a definição de divisibilidade, propriedades, o Teorema de Eudoxius e o Algoritmo da Divisão, o qual serão ferramentas importantes para a construção de resultados referentes à prova dos noves. Para isso, utilizaremos como base a bibliografia [16].

Definição 2.1. Sejam a e $b \in \mathbb{Z}$, dizemos que *a divide b*, e denotamos por $a|b$ se existir um número inteiro c tal que $b = ac$. Nesse caso, diremos também que a é um divisor de b, ou ainda, que b é um múltiplo de a ou que b é divisível por a.

Se a não divide b, escrevemos $a \nmid b$.

A partir da Definição 2.1 apresentaremos algumas propriedades de divisibilidade.

Proposição 2.2. *Se a, b e c são números inteiros, $a|b$ e $b|c$, então $a|c$.*

Demonstração. Sejam $a, b, c \in \mathbb{Z}$. Como $a|b$, existe $m \in \mathbb{Z}$ tal que

$$b = am. \tag{2.1}$$

Da mesma forma, como $b|c$, existe $n \in \mathbb{Z}$ tal que

$$c = bn. \tag{2.2}$$

Substituindo (2.1) em (2.2), temos

$$c = bn = (am)n = a(mn)$$

Portanto, $a|c$.

$\blacksquare$

Exemplo 2.3. Como $3|18$ e $18|108$, e pela Proposição (2.2), temos que $3|108$.

Proposição 2.4. *Se a, b, c, m e n são números inteiros, $c|a$ e $c|b$, então $c|(ma + nb)$.*

Demonstração. Sejam a, b, c, m e $n \in \mathbb{Z}$. Temos que se $c|a$, existe $x \in \mathbb{Z}$ tal que

$$a = cx. \tag{2.3}$$

Também que se $c|b$, existe $y \in \mathbb{Z}$ tal que

$$b = cy. \tag{2.4}$$

Multiplicando (2.3) por m e (2.4) por n, respectivamente, temos

$$am = (cx)m \tag{2.5}$$

e

$$bn = (cy)n. \tag{2.6}$$

Somando as duas últimas equações, encontramos

$$am + bn = cxm + cyn \Rightarrow$$

$$am + bn = c(xm + yn). \tag{2.7}$$

Logo, por (2.7) concluímos que $c|(am + bn)$.

$\blacksquare$

Exemplo 2.5. Como $7|21$ e $7|42$, então $7|(8 \cdot 21 - 7 \cdot 42)$, ou seja, $7|126$.

Proposição 2.6. *Sejam $a, b, c \in \mathbb{Z}$ tais que $a|(b \pm c)$. Então,*

$$a|b \Leftrightarrow a|c.$$

Demonstração. Suponhamos que $a|(b+c)$. Então, existe $x \in \mathbb{Z}$ tal que $b+c = xa$. Se $a|b$, existe $y \in \mathbb{Z}$ tal que $b = ya$. Substituindo a última igualdade em $b+c = xa$, temos $ya + c = xa$. Daí, $ya + (-ya) + c = xa + (-ya)$, ou seja,$c = a(x-y)$, logo $a|c$. De forma análoga, provamos a implicação contrária.

Como $a|(b+c)$, então existe $m \in \mathbb{Z}$ tal que $b+c = ma$. Se $a|c$, existe $n \in \mathbb{Z}$ tal que $c = na$. Substituindo a última igualdade em $b+c = ma$, temos $b + an = ma$. Segue que, $b + an + (-an) = ma + (-an)$, ou seja,$b = a(m-n)$, logo $a|b$.

■

Teorema 2.7. *Sejam a, d, n números inteiros. As seguintes propriedades valem:*

(a) $n|n$.

(b) $d|n \Rightarrow ad|an$.

(c) $ad|an$ *e* $a \neq 0 \Rightarrow d|n$.

(d) $1|n$.

(e) $n|0$.

(f) $d|n$ *e* $n \neq 0 \Rightarrow |d| \leq |n|$.

(g) $d|n$ *e* $n|d \Rightarrow |d| = |n|$.

(h) $d|n$ *e* $d \neq 0 \Rightarrow (n/d)|n$.

Demonstração.

(a) Existe $1 \in \mathbb{Z}$ tal que $n = 1 \cdot n$, para todo $n \in \mathbb{Z}$. Logo, $n|n$, para todo $n \in \mathbb{Z}$.

(b) Se $d|n$, existe $c \in \mathbb{Z}$ tal que $n = dc$. Multiplicando esta igualdade por a, temos $an = adc$. Logo, pela associatividade da multiplicação em $\mathbb{Z}$, temos que $an = (ad)c$ e, portanto, $ad|an$.

(c) Se $ad|an$, existe $c \in \mathbb{Z}$ tal que $an = c(ad)$, ou seja, $an = acd$. Logo, $an - acd = 0$ implica que $a(n-cd) = 0$. Por hipótese, $a \neq 0$ e como um número inteiro não possui divisores de zero, temos que $n - cd = 0$, ou seja,$n = cd$. Logo, $d|n$.

(d) Como 1 é o elemento neutro da multiplicação, temos que $n = 1 \cdot n$, para todo $n \in \mathbb{Z}$.

(e) Como, $0 = 0 \cdot n$, para todo $n \in \mathbb{Z}$, $n|0$.

(f) Se $d|n$, existe $m \in \mathbb{Z}$ tal que $n = dm$. Então, $|n| = |dm| = |n| = |d|\,|m|$[1]. Como $n \neq 0$, temos $m \neq 0$ e, portanto, $|m| \geq 1$, logo $|n| = |d|\,|m| \geq |d|$. Portanto, $|d| \leq |n|$.

(g) Se $d|n$, existe $c \in \mathbb{Z}$ tal que

$$n = dc. \tag{2.8}$$

Se $n|d$, existe $r \in \mathbb{Z}$ tal que

$$d = nr. \tag{2.9}$$

Substituindo (2.8) em (2.9), temos

$$d = nr \Rightarrow d = (dc)r \Rightarrow |cr| = 1 \Rightarrow |c| = 1 \text{ e } |r| = 1.$$

Assim, $|d| = |d|\,|c|\,|r| = |d| = |n|\,|r|$. Logo, $|d| = |n|$.

(h) Se $d|n$, existe $r \in \mathbb{Z}$ tal que $n = dr$. E, portanto, $\dfrac{n}{d} \in \mathbb{Z}$. Como $\left(\dfrac{n}{d}\right) \cdot d = n$, segue que $\left(\dfrac{n}{d}\right)|n$.

■

As proposições, a seguir, apresentam grande utilidade na resolução de exercícios referentes à divisibilidade e serão demonstradas usando indução sobre n.

Proposição 2.8. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Então, $a - b$ divide $a^n - b^n$.*

Demonstração. Seja $P(n) : a - b|a^n - b^n$.

$(i.)$ $P(1)$ é verdadeira, pois $a^1 - b^1 = a - b$ e $a - b|a - b$, já que $a - b = 1(a - b)$.

$(ii.)$ Suponhamos que $P(k)$ é verdadeira, para algum $k \in \mathbb{N}$, ou seja,

$P(k) : a - b|a^k - b^k$, ou seja, $a^k - b^k = x(a - b), x \in \mathbb{Z}$ (HI).

Queremos mostrar que $P(k + 1)$ é verdadeira. Notemos que,

$$\begin{aligned} P(k+1) = a^{k+1} - b^{k+1} &= a^k \cdot a - b^k \cdot b \\ &= a^k \cdot a - b^k \cdot b + a^k \cdot b - a^k \cdot b \end{aligned}$$

[1] Para mais informações sobre definição ou propriedades básicas do módulo, veja a bibliografia [9], p.10.

$$
\begin{aligned}
&= a^k(a-b) + b\underbrace{(a^k - b^k)}_{(HI)} \\
&= a^k(a-b) + b(x(a-b)) \\
&= (a-b)(a^k + bx) \\
&= (a-b)z, z \in \mathbb{Z}.
\end{aligned}
$$

A última igualdade mostra que $P(k+1)$ é verdadeira. Pelo Princípio de Indução Finita, $P(n)$ é verdadeira, para todo $n \in \mathbb{N}$.

■

Exemplo 2.9. Todo número da forma $10^n - 1$ é divisível por 9.

Solução. Utilizando a Proposição 2.8, com $a = 10$, $b = 1$, resulta que $a - b = 10 - 1 = 9$, então 9 divide $10^n - 1^n = 10^n - 1$.

Proposição 2.10. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$. Então $a + b$ divide $a^{2n+1} + b^{2n+1}$.*

Demonstração. Seja $P(n) : a + b | a^{2n+1} + b^{2n+1}$, onde $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$.

($i.$) $P(0)$ é verdadeira, pois $a^{2\cdot 0+1} + b^{2\cdot 0+1} = a + b$ e $a + b | a + b$, já que $a + b = 1(a + b)$.

($ii.$) Suponhamos que $P(k)$ verdadeira, para algum $k \in \mathbb{N}$, ou seja,

$P(k) : a + b | a^{2k+1} + b^{2k+1}$, ou seja, $a^{2k+1} + b^{2k+1} = x(a + b), x \in \mathbb{Z}$ (HI).

Queremos mostrar que $P(k+1)$ é verdadeira. Notemos que,

$$
\begin{aligned}
P(k+1) &= a^{2(k+1)+1} + b^{2(k+1)+1} = a^{2k+2+1} + b^{2k+2+1} \\
&= a^{2k+1} \cdot a^2 + b^{2k+1} \cdot b^2 + a^{2k+1} \cdot b^2 - a^{2k+1} \cdot b^2 \\
&= b^2(\underbrace{a^{2k+1} + b^{2k+1}}_{(HI)}) + a^{2k+1}(a^2 - b^2) \\
&= b^2x(a+b) + a^{2k+1}(a+b)(a-b) \\
&= (a+b)\left[b^2x + a^{2k+1}(a-b)\right] \\
&= (a+b)z, z \in \mathbb{Z}.
\end{aligned}
$$

A última igualdade nos mostra que $P(k+1)$ é verdadeira. Pelo Princípio de Indução Finita, $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

■

Proposição 2.11. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Então $a+b$ divide $a^{2n} - b^{2n}$.*

Demonstração. Seja $P(n) : a+b | a^{2n} - b^{2n}$, onde $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$.

1) $P(1)$ é verdadeira, pois $a^{2\cdot 1} - b^{2\cdot 1} = a^2 - b^2 = (a-b)(a+b)$, logo, $(a+b)|(a^2 - b^2)$.

2) Suponhamos que $P(k)$ é verdadeira, para algum $k \in \mathbb{N}$, ou seja, $P(k) : a+b|a^{2k} - b^{2k}$. Então $a^{2k} - b^{2k} = x(a+b), x \in \mathbb{Z}$ (HI).

Queremos mostrar que $P(k+1)$ é verdadeira. Notemos que,

$$\begin{aligned}
P(k+1) &= a^{2(k+1)} - b^{2(k+1)} = a^{2k+2} - b^{2k+2} \\
&= a^{2k} \cdot a^2 - b^{2k} \cdot b^2 \\
&= a^{2k} \cdot a^2 - b^{2k} \cdot b^2 + a^{2k}b^2 - a^{2k}b^2 \\
&= b^2(\underbrace{a^{2k} - b^{2k}}_{(HI)}) + a^{2k}(a^2 - b^2) \\
&= b^2 x(a+b) + a^{2k}(a+b)(a-b) \\
&= (a+b)\left[b^2 x + a^{2k}(a-b)\right] \\
&= (a+b)z, z \in \mathbb{Z}.
\end{aligned}$$

A última igualdade mostra que $P(k+1)$ é verdadeira. Pelo Princípio de Indução Finita, $P(n)$ é verdadeira, para todo $n \in \mathbb{N}$.

■

Antes de introduzirmos o algoritmo da divisão, enunciaremos o Teorema de Eudoxius [2].

Teorema 2.12 (Teorema de Eudoxius)**.** *Dados a e b números inteiros com $b \neq 0$, então a é múltiplo de b ou se encontra entre dois múltiplos consecutivos de b, isto é, correspondendo a cada par de inteiros a e $b \neq 0$ existe um inteiro q tal que, para $b > 0$,*

$$qb \leq a < (q+1)b \tag{2.10}$$

e para $b < 0$,

$$qb \leq a < (q-1)b. \tag{2.11}$$

[2]Segundo Santos, 2009, [16] este teorema costuma ser erroneamente atribuído a Arquimedes e chamado "Princípio de Arquimedes".

Demonstração. Sejam $a > 0$ e $b > 0$ inteiros (prova-se de forma análoga os casos em que $a < 0$ ou $b < 0$). Temos dois casos a considerar:

- Se $a = qb$, para algum $q \in \mathbb{Z}$, então a é múltiplo de b e nada temos a provar.

- Se $a \neq qb$, então, pelo Princípio da Boa Ordenação, existe $x \in \mathbb{Z}$ menor inteiro que satisfaz $a < xb$.

Como consequência, $q = (x-1)b < a$. Portanto, $(x-1)b < a$ e $a < xb$ implicam que $(x-1)b < a < xb$. Sendo $q = x - 1$ e substituindo na última desigualdade, encontramos $qb \leq a < (q+1)b$.

∎

Teorema 2.13 (Algoritmo da divisão)**.** *Dados dois inteiros a e b, $b > 0$, existe um único par de inteiros q e r tais que*

$$a = qb + r,$$

*com $0 \leq r < b$ (q é chamado de **quociente** e r de **resto** da divisão de a por b).*

Demonstração. (Existência) Pelo Teorema de Eudoxius, se $b > 0$ existe q tal que $qb \leq a < (q+1)b$, o que implica que $0 \leq a - qb$ e $a - qb < b$, pois $0 \leq a - qb < qb + b - qb = b$. Logo, sendo $r = a - qb$, garantimos a existência de q e r.

(Unicidade) Suponhamos que existem q_1, q_2, r_1 e r_2 inteiros tais que $a = q_1 b + r_1$ e $a = q_2 b + r_2$, com $0 \leq r_1 < b$ e $0 \leq r_2 < b$.

Disto, $q_1 b + r_1 = q_2 b + r_2$, donde $b(q_1 - q_2) + r_1 - r_2 = 0$. Logo, $b(q_1 - q_2) = r_2 - r_1$, portanto $b | r_2 - r_1$.

Como, $0 \leq r_1, r_2 < b$, temos $|r_2 - r_1| < b$, e portanto, como $b | r_2 - r_1$, temos que $r_2 - r_1 = 0$. Logo, $r_2 = r_1$. Portanto, $q_1 b = q_2 b$, donde $q_2 = q_1$, uma vez que $b \neq 0$. Assim, a unicidade está provada.

∎

Ressaltamos que é possível enunciar o Teorema 2.13 com $b \in \mathbb{Z}$, $b \neq 0$, e não somente com a restrição de que $b > 0$. Para isto, basta utilizar a equação (2.11) e encontrar q e r também para $b < 0$.

Capítulo 3

O sistema de numeração decimal

Neste capítulo, apresentaremos as propriedades do sistema decimal posicional, o qual utilizamos para representar os números inteiros.

O estudo dessa seção justifica-se, pois os números e sua representação decimal são o nosso objeto de estudo e são necessários para posterior demonstração da prova dos nove para as quatro operações básicas. Utilizaremos como base as bibliografias [9] e [16].

3.1 A representação dos números inteiros

No sistema decimal, todo número inteiro pode ser representado utilizando os algarismos $1, 2, 3, 4, 5, 6, 7, 8, 9$, juntamente com o 0 (zero), o qual representa a ausência de algarismo. Cada algarismo tem um peso dependendo da posição que ele ocupa. Por isso, dizemos que o nosso sistema de numeração é posicional. E por serem dez algarismos, nosso sistema também é chamado decimal, veja [9].

Vamos fazer uso de um exemplo para melhor compreender a representação de um número na base 10.

Exemplo 3.1. Consideremos o número 37.406 no sistema decimal.

Notemos que o número 37.406 pode ser representado da seguinte maneira,

$37.406 = 3 \cdot 10^4 + 7 \cdot 10^3 + 4 \cdot 10^2 + 0 \cdot 10^1 + 6 \cdot 10^0$.

Assim, o algarismo 6, da extrema direita, tem peso 1 (ou 10^0), o algarismo 0, seguinte, tem peso 10^1, o próximo algarismo, o 4, tem peso 10^3, e assim, sucessivamente.

Observemos, também, que o 0 ocupa a segunda casa e representa a ausência da potência 10^1.

Cada algarismo possui uma ordem contada da direita para a esquerda. Logo, no exemplo acima, o 6 é de primeira ordem, o 7 é de quarta ordem, o 4 é de terceira ordem.

A cada terna de ordens, contadas da direita para a esquerda, forma-se uma classe. Os nomes das primeiras classes e ordens são:

Classe das Unidades: compreende as unidades, dezenas e centenas, que representam a primeira, segunda e terceira ordem, respectivamente.

Classe do Milhar: compreende as unidades de milhar, dezenas de milhar e centenas de milhar, que representam a quarta, quinta e sexta ordem, respectivamente.

Classe do Milhão: compreende as unidades de milhão, dezenas de milhão e centenas de milhão, que representam a sétima, oitava e nona ordem, respectivamente.

Note também que o número 37406 pode ser lido como: 6 unidades, 0 dezenas, 4 centenas, 7 unidades de milhar e 3 dezenas de milhar, pois cada posição corresponde a uma ordem nomeada como foi descrito.

Seja $n > 0$ inteiro, tal que $n = r_k r_{k-1} \dots r_1 r_0$, onde $k \geq 0$ e $r_k, r_{k-1}, \dots, r_1, r_0$ são os algarismos que compõem n . Sua representação na forma expandida será escrita da forma $n = r_k 10^k + r_{k-1} 10^{k-1} + \dots + r_1 10^1 + r_0$, onde $k \geq 0$ e $r_k \neq 0$.

É importante ressaltar que é possível construir sistemas de numeração posicionais em qualquer base $b > 1$, $b \in \mathbb{Z}$. E um importante resultado será apresentado, o qual demonstra que todo inteiro $n > 0$ pode ser representado de forma única por um sistema de numeração posicional. Neste teorema apresentamos a expansão de um inteiro positivo n para uma base b, $b > 1$, $b \in \mathbb{Z}$. O que vale para o nosso sistema de numeração decimal, cuja base é $b = 10$. Vale mencionar que este teorema é uma aplicação da divisão euclidiana.

Teorema 3.2. *Seja b um inteiro positivo maior do que 1. Então, todo inteiro positivo n pode ser escrito de maneira única da forma*

$$n = r_k b^k + r_{k-1} b^{k-1} + \dots + r_1 b^1 + r_0, \tag{3.1}$$

onde $k \geq 0$, $r_k \neq 0$ e $0 \leq r_i < b$, $i = 0, 1, \dots, k$.

Demonstração. Inicialmente, consideremos $0 < n < b$. Assim, para escrever n da forma enunciada, basta tomar $k = 0$ e $r_0 = n$. É possível escrever qualquer inteiro $0 < n < b$ da forma (3.1), tomando $n = r_0$. A unicidade da escrita de n, nesse caso, fica evidente, pois escolhemos $r_0 = n$. Vamos demonstrar utilizando indução sobre n.

Suponhamos o resultado válido para todo $n' < n$, onde $n \geq b$. Vamos mostrar que é válido para todo $n \in \mathbb{N}$.

Pelo algoritmo da divisão, e supondo $0 < q < n$, temos pela divisão euclidiana que existem q e r únicos, tais que

$$n = bq + r, \tag{3.2}$$

com $0 \leq r < b$.

Pela hipótese de indução, temos que se $0 < q < n$, existem $r_1, r_2, \ldots, r_{k'+1} < b$ unicamente determinados, tais que

$$q = r_1 + r_2 b + \ldots + r_{k'+1} b^{k'}. \tag{3.3}$$

Substituindo (3.3) em (3.2), obtemos

$$n = b(r_1 + r_2 b + \ldots + r_{k'+1} b^{k'}) + r = r_1 b + r_2 b^2 + \ldots + r_{k'+1} b^{k'+1} + r.$$

Sendo $r = r_0$ e $r_{k'+1} = r_k$, a igualdade é verdadeira para todo $n > 0$ e, portanto, está provada.

$\blacksquare$

A representação $n = r_k b^k + r_{k-1} b^{k-1} + \ldots + r_1 b^1 + r_0$ é denominada *expansão relativa à base b*. Como foi dito anteriormente, quando $b = 10$ (caso do nosso sistema de numeração) chamamos de expansão decimal.

Agora que foi provado que essa representação é única, vamos fazer uso da mesma para a demonstração do critério de divisibilidade por 9, isto porque, a prova dos nove tem como base o critério de divisibilidade por 9, como veremos adiante.

A seguir, temos o resultado referente a este critério de divisibilidade.

Proposição 3.3. *Seja $n = r_k \ldots r_2 r_1 r_0$ um número representado no sistema decimal. Então n é divisível por 9 se, e somente se, $r_k + r_{k-1} + \ldots + r_1 + r_0$ for divisível por 9.*

Demonstração. Seja

$$n = r_k \dots r_2 r_1 r_0. \tag{3.4}$$

Também podemos representá-lo da forma

$$n = r_k 10^k + \dots + r_2 10^2 + r_1 10^1 + r_0. \tag{3.5}$$

Subtraindo a expressão $r_k + r_{k-1} + \dots + r_1 + r_0$ da equação (3.5), temos $n - (r_k + \dots + r_1 + r_0) = r_k 10^k + \dots + r_1 10 + r_0 - r_k - \dots - r_1 - r_0 = r_k(10^k - 1) + \dots + r_1(10 - 1) + r_0 - r_0$.

Logo $n - (r_k + \dots + r_1 + r_0) = r_k(10^k - 1) + \dots + r_1(10 - 1)$.

Observemos que os termos da direita são todos divisíveis por 9 [1], assim, podemos representar esta última igualdade como

$n - (r_k + \dots + r_1 + r_0) = 9q$, $q \in \mathbb{Z}$, isto é,

$n = (r_k + \dots + r_1 + r_0) + 9q$, de onde o resultado segue devido às Proposições 2.4 e 2.6.

■

Exemplo 3.4. O número 2 345 688 é divisível por 9, pois $2 + 3 + 4 + 5 + 6 + 8 + 8 = 36$ que é divisível por 9.

Observemos que o critério de divisibilidade por 9 pode ser usado de forma "iterativa", pois se ao somarmos os algarismos ainda obtivermos um resultado consideravelmente grande para sabermos mentalmente se o número é divisível por 9, podemos usar o critério de divisibilidade novamente, quantas vezes nos for conveniente até reduzir o valor.

Tomemos novamente o exemplo anterior, o qual dizia que o número 2 345 679 era divisível por 9. Aplicando o critério de divisibilidade por 9, temos

$2 + 3 + 4 + 5 + 6 + 8 + 8 = 36$, e $3 + 6 = 9$, que é divisível por 9.

É importante mencionar que existem outros critérios de divisibilidade por outros números, mas o critério de divisibilidade por 9 é o que tem relevância para o nosso trabalho e por isso é o que foi apresentado.

[1] pela Proposição 2.8 e Exemplo 2.9, todo número da forma $10^n - 1$, $n \in \mathbb{N}$, é divisível por 9.

Capítulo 4

Congruências e divisibilidade

Ao fundamentarmos a prova dos noves ou a regra dos “noves fora”, faz-se interessante apresentar os principais resultados referentes à congruência módulo m, ou à aritmética dos restos de uma divisão por $m \in \mathbb{Z}$, $m > 1$.

Para isso, utilizaremos como base a bibliografia [4]. Como bibliografia complementar utilizamos [16], [9] e [6].

Vamos iniciar definindo a relação de congruência.

Definição 4.1. Sejam $a, b, m \in \mathbb{Z}$ e $m > 1$. Dizemos que a é congruente a b módulo m, se os restos das divisões a e b por m são iguais, e denotamos por $a \equiv b \pmod{m}$.

Caso a e b não deixam o mesmo resto quando divididos por m, dizemos que a e b não são congruentes, ou a e b são incongruentes e escrevemos $a \not\equiv \pmod{m}$.

Observamos que, quando $m = 1$, quaisquer dois inteiros são sempre congruentes módulo 1, e também se $a \equiv b \pmod{m}$, então $a \equiv b \pmod{-m}$. Por isso, supomos $m \in \mathbb{Z}$ e $m > 1$ [7].

A partir da definição 4.1, podemos enunciar o seguinte resultado.

Proposição 4.2. *Sejam $a, b, m \in \mathbb{Z}$ e $m > 1$. Temos que $a \equiv b \pmod{m}$ se, e somente se, $m | a - b$.*

Demonstração.

Se $a \equiv b \pmod{m}$ então existem q_1, q_2, $r \in \mathbb{Z}$, $0 \leq r < m$, tais que

$$a = q_1 m + r \tag{4.1}$$

e

$$b = q_2 m + r. \tag{4.2}$$

Subtraindo membro a membro (4.2) de (4.1), temos

$a - b = q_1 m + r - q_2 m - r = m(q_1 - q_2)$, o que implica que $m | a - b$.

Reciprocamente, suponhamos que $m | a - b$ e sejam r_1 seja o resto da divisão de a por m, e r_2 seja o resto da divisão de b por m, onde r_1 e r_2 são distintos e $0 \leq r_1, r_2 < m$. Dessa forma,

$$a = mq_1 + r_1 \tag{4.3}$$

e

$$b = mq_2 + r_2. \tag{4.4}$$

Subtraindo (4.4) de (4.3) membro a membro, obtemos

$$a - b = mq_1 + r_1 - (mq_2 + r_2) = m(q_1 - q_2) + (r_1 - r_2).$$

Pela Proposição 2.6, $m | (r_1 - r_2)$. Logo, $m || r_1 - r_2|$ o que implica que $|r_1 - r_2| = 0$, pois $0 \leq r_1, r_2 < m$. Logo, $r_1 = r_2$ e, então, $a \equiv b \pmod m$.

■

A congruência módulo m é uma relação de equivalência, pois satisfaz as propriedades reflexiva, simétrica e transitiva, conforme a proposição a seguir.

Proposição 4.3 (Relação de equivalência.)**.** *Sejam $a, b, c, m \in \mathbb{Z}$, $m > 1$. As seguintes sentenças são verdadeiras:*

(i) $a \equiv a \pmod m$*;*

(ii) Se $a \equiv b \pmod m$*, então* $b \equiv a \pmod m$*;*

(iii) Se $a \equiv b \pmod m$ *e* $b \equiv c \pmod m$*, então* $a \equiv c \pmod m$*.*

Demonstração.

(i) Como $m | 0$, para todo $m > 1$, temos que $m | (a - a)$. Assim, pela Proposição 4.2 temos que $a \equiv a \pmod m$.

(ii) Se $a \equiv b \pmod{m}$, então $m|(a-b)$, ou seja $m|-(a-b)$. Logo $m|b-a$, portanto, $b \equiv a \pmod{m}$.

(iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $m|(a-b)$ e $m|(b-c)$. Logo, da Proposição 2.4, temos que $m|(a-b)+(b-c)$, implicando que $m|(a-c)$.

$\blacksquare$

Além da relação de equivalência, a congruência possui os seguintes resultados, importantes para o desenvolvimento deste trabalho.

Proposição 4.4. *Sejam a, b e $m > 1$ inteiros. As seguintes afirmações são verdadeiras:*

(i) *$a \equiv b$ (mod m), se, e somente se, o resto da divisão de a por m e o resto da divisão de b por m é r.*

(ii) *Se r é o resto da divisão de a por m, então $a \equiv r$ (mod m). Reciprocamente, se $a \equiv r$ (mod m) e $0 \leq r < m$, então r é o resto da divisão de a por m.*

Demonstração. *(i)* Sejam $a = mq_1 + r_1$ e $b = mq_2 + r_2$, onde q_1, q_2, r_1, r_2 são números inteiros, com $0 \leq r_1, r_2 < m$. Se $a \equiv b \pmod{m}$, então $m|(mq_1 - mq_2) + (r_1 - r_2)$. Mas, $m|(q_1 - q_2)m + (r_1 - r_2)$, ou seja, $m|(r_1 - r_2)$. Podemos assumir, sem perda de generalidade que $r_2 \leq r_1$. Como $0 \leq r_1 - r_2 < m$, temos $r_1 - r_2 = 0$. Logo, $a \equiv b \pmod{m}$. Portanto, $r_1 = r_2$.

(ii) Seja $a = mq + r$, com $q, r \in \mathbb{Z}$ e $0 \leq r < m$. Então, $a - r = mq$, o que implica que $m|a-r$, se, e somente se, $a \equiv r \pmod{m}$.

Reciprocamente, se $a \equiv r \pmod{m}$, então $m|(a-r)$. Logo, $a-r = mq$, ou seja, $a = mq+r$. Como $0 \leq r < m$, pelo Algoritmo da Divisão, temos que o resto da divisão é único. Logo, r é o resto da divisão de a por m.

$\blacksquare$

Teorema 4.5. *Sejam $a, b, c, d, m \in \mathbb{Z}$, $m > 1$ tais que $a \equiv b$ (mod m), então*

(i) *Se $a \equiv b$ (mod m) e $c \equiv d$ (mod m) então, $a + c \equiv b + d$ (mod m);*

(ii) Se $a \equiv b$ (mod m) e $c \equiv d$ (mod m) então $ac \equiv bd$ (mod m);

(iii) Se n é um inteiro positivo e $a \equiv b$ (mod m), então $a^n \equiv b^n$ (mod m).

Demonstração.

(i) Se $a \equiv b \pmod m$ e $c \equiv d \pmod m$, então $m|(a-b)$ e $m|(c-d)$. Logo, por (2.4), $m|(a-b)+(c-d)$, o que implica que $m|(a+c)-(b+d)$ e, então, $a+c \equiv b+d \pmod m$.

(ii) Se $a \equiv b \pmod m$ e $c \equiv d \pmod m$, então $m|(a-b)$ e $m|c-d$. Daí, $m|c(a-b)$ e $m|b(c-d)$. Então, $m|ac-bc$ e $m|bc-bd$. Pela Proposição 2.4, $m|ac-bc+bc-bd$, ou seja, $m|ac-bd$. Logo $ac \equiv bd \pmod m$.

iii. Vamos provar utilizando indução sobre n. Devemos mostrar que
$P(n) : a \equiv b \pmod m \Longrightarrow a^n \equiv b^n \pmod m, n \in \mathbb{N}$ é verdadeira.

Primeiramente, P(1) é verdadeira, pois $a^1 \equiv b^1 \pmod m$, ou seja, $a \equiv b \pmod m$, por hipótese.

Suponhamos que $P(k)$ verdadeira, para algum $k \in \mathbb{N}$, ou seja,
$P(k) : a \equiv b \pmod m \Longrightarrow a^k \equiv b^k \pmod m$ (HI).

Queremos mostrar que $P(k+1)$ é verdadeira. Por hipótese, $a \equiv b \pmod m$. Pelo item *(ii.)*, juntamente com a (HI), temos: $\begin{cases} a \equiv b \pmod m \\ a^k \equiv b^k \pmod m \end{cases} \Longrightarrow a \cdot a^k \equiv b \cdot b^k \pmod m \Longrightarrow$ $a^{k+1} \equiv b^{k+1} \pmod m$.

Logo $P(k+1)$ é verdadeira. Pelo princípio de indução finita, $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

■

Corolário 4.6. *Se a, b e $m > 1$ são inteiros e $a \equiv b$ (mod m), então $m|a$ se, e somente se $m|b$.*

Demonstração. Se $a \equiv b \pmod m$, então $m|(b-a)$. Pela Proposição 2.6, segue que $m|a$ se, e somente se, $m|-b \Longrightarrow m|b$.

■

Uma aplicação direta dos resultados sobre congruência é na demonstração dos critérios de divisibilidade. Nesta seção, demonstraremos o critério de divisibilidade por 9 (já demonstrado no capítulo anterior) fazendo uso das congruências e suas propriedades.

Proposição 4.7. *Seja $n = r_k \ldots r_1 r_0$ um número inteiro representado no sistema decimal, onde $r_k, \ldots, r_1, r_0 \in \mathbb{Z}$ são os algarismos que compõem n. Então n é divisível por 9 se, e somente se, $r_k + \ldots + r_1 + r_0$ também for divisível por 9.*

Demonstração. Seja $n = r_k \ldots r_1 r_0$ um número inteiro escrito na base decimal. Pelo Teorema 3.2, temos que

$$n = 10^k r_k + \ldots + 10 r_1 + r_0. \tag{4.5}$$

Agora, pela Proposição 2.8 e pelo Exemplo 2.9, temos que $9|(10^k - 1)$, isto é, $10 \equiv 1 \pmod 9$ e pelo Teorema 4.5(ii), $10^i \equiv 1 \pmod 9$ para qualquer inteiro positivo i.

Assim, utilizando o Teorema 4.5(ii) temos que $r_i 10^i \equiv r_i \pmod 9$, para todo $i = 0, 1, 2, \ldots, k$.

Assim, pelo Teorema 4.5(i),

$$r_k 10^k + r_{k-1} 10^{k-1} + \ldots + r_1 10^1 + r_0 \equiv r_k + r_{k-1} + \ldots + r_1 + r_0 \pmod 9.$$

Logo, pelo Corolário 4.6, $9|n$ se, e somente se, $9|r_k + r_{k-1} + \ldots + r_1 + r_0$.

$\blacksquare$

Capítulo 5

A Prova dos Noves

A prova dos noves é uma regra que possibilita verificar se uma operação aritmética foi realizada corretamente, mais especificamente, é usada para identificar erros em operações básicas (adição, subtração, multiplicação e divisão).

Não foram encontradas referências que apontam a origem da prova dos noves e a época em que esta foi inserida nos currículos escolares. O que se encontram são indícios de que esta regra é um conceito de séculos passados.

A prova dos noves já era mencionada na primeira aritmética árabe que se conhece, a de al-Khowârizmî, que viveu no século IX. Após essa primeira aritmética seguiram-se outras, e todas apresentavam regras para efetuar cálculos baseadas em algoritmos hindus e a regra para verificação de cálculo, já denominada na época como processo dos "noves foras" ou a prova dos noves, veja [5].

Antes da popularização do uso das calculadoras, a prova dos noves era muito utilizada por comerciantes, contabilistas e economistas com o objetivo de verificar se existem erros nas quatros operações básicas [3].

A prova dos noves era um conteúdo trabalhado nas escolas e por ser uma regra simples de ser aplicada, podia ser ensinada aos alunos, sem se preocupar com a teoria que existe por trás destas regras e seu embasamento, veja [3].

Na bibliografia [2], a autora relata a própria história de que, quando iniciou a universidade e começou a ministrar aulas, ela ensinava os alunos a decorar a tabuada e realizar as operações básicas com números naturais. Além de efetuar as operações básicas, ela também ensinava a prova real e a prova dos noves, que também apareciam em livretos de tabuadas vendidos no comércio. Ela relata também que a prova dos noves ainda é utilizada por alguns comerciantes locais.

Atualmente, a prova dos noves caiu em desuso e não é mais ensinada nas escolas, e hoje, poucas pessoas sabem do que se trata. A inserção das calculadoras em sala de aula fez com que a prova dos noves fosse deixada de lado, conforme relata em [3]. Isso, entretanto, não minimiza sua importância no que diz sentido ao desenvolvimento do cognitivo e do cálculo mental, por exemplo.

Ao falarmos do desuso da prova dos noves, é interessante mencionar a bibliografia [17], onde a autora resgata, por meio de uma história fictícia o que são os "noves fora" e a prova dos noves, como e porque ela funciona, tornando uma boa bibliografia para quem deseja conhecer como funciona a prova dos noves.

Outra bibliografia relevante é [10], que faz uma análise das diferentes abordagens da prova dos noves em livros didáticos de aritmética, editados no período de 1890 à 1970.

Neste capítulo, apresentaremos a regra dos "noves fora", o que é a prova dos noves e como ela funciona por meio de demonstrações de resultados que são as bases dessa prova. No que se refere à prova dos noves, faremos apenas para o caso dos números naturais, uma vez que os resultados podem ser estendidos facilmente para os números inteiros.

Vamos iniciar apresentando o conceito da regra dos "noves fora". Para este capítulo, utilizamos como base [6] e [3].

5.1 A regra dos "noves fora" e a prova dos noves

Definição 5.1. Seja n um número natural. Retirar os "noves fora" de um natural n significa determinar o resto de sua divisão por 9.

Ou, em outras palavras podemos dizer que retirar os "noves fora" de n significa retirar o maior múltiplo de 9 de n.

Exemplo 5.2. 13 "noves fora" 4, pois $13 - 9 = 4$, ou ainda, podemos dizer que 4 é o resto da divisão de 13 por 9, isto é, $13 = 1 \cdot 9 + 4$.

Exemplo 5.3. 57 "noves fora" 3, pois $57 - 6 \cdot 9 = 3$, isto é, 3 é o resto da divisão de 57 por

9, ou seja, $57 = 6 \cdot 9 + 3$.

No entanto, existe uma maneira mais prática para determinar os “noves fora” de um número, sem precisar efetuar a divisão deste número por 9, como veremos a seguir. Esta maneira prática, tem como base o critério de divisibilidade por 9.

No Capítulo 3, enunciamos e provamos o critério de divisibilidade por 9, o qual afirma que um número n é divisível por 9 se, e somente se, a soma de seus algarismos também o for.

De maneira equivalente, temos que o resto da divisão de um número por 9 é igual ao resto obtido pela divisão por 9 da soma dos seus algarismos, isto é, os “noves fora” de um número $n = r_k r_{k-1} \ldots r_1 r_0$ é igual aos “noves fora” de $r_k + r_{k+1} + \ldots + r_1 + r_0$. Logo, encontrar os “noves fora” de um natural n equivale a encontrar os “noves fora” da soma dos algarismo de n, o qual é mais utilizada por ser mais prática.

Na proposição a seguir, mostraremos a validade desse resultado.

Proposição 5.4. *Seja $n = r_k r_{k-1} \ldots r_2 r_1 r_0$ um número natural, onde $r_k, r_{k-1}, \ldots, r_2, r_1, r_0$ são os algarismos que compõem n. Então, o resto da divisão de n por 9 é igual ao resto obtido pela divisão de $n' = r_k + r_{k-1} + \ldots + r_1 + r_0$ por 9.*

Demonstração. Pelo Algoritmo da Divisão, podemos determinar únicos q, q'', r, r'' com $0 \leq r, r'' < 9$ tais que $n = 9q + r$ e $n' = 9q'' + r''$.

Agora, seja $n = 10^k r_k + 10^{k-1} r_{k-1} + \ldots + 10^1 r_1 + r_0$ a expansão de n na forma decimal. Subtraindo n' de n temos,

$n - (r_k + \ldots + r_1 + r_0) = r_n(10^n - 1) + \ldots + r_1(10 - 1)$.

Observemos que os termos da direita são todos divisíveis por 9 [1], então podemos representar esta última igualdade como

$n - (r_k + \ldots + r_1 + r_0) = 9q'$ (*), $q' \in \mathbb{N}$,

Substituindo $n = 9q + r$ e $n' = 9q'' + r''$ em (*), temos,

$n - (9q'' + r'') = 9q'$, ou seja, $n = 9q' + 9q'' + r''$. Logo, $9q + r = 9\underbrace{(q' + q'')}_{q'''} + r''$.

[1]todo número da forma $10^n - 1$, $n \in \mathbb{N}$, é divisível por 9.

Pelo Algoritmo da Divisão, $0 \leq r, r'' < 9$ e q, q''' são únicos, logo $r = r''$, ou seja, o resto da divisão de n por 9 é igual ao resto da divisão de n' por 9.

■

Nos exemplos a seguir, podemos observar que o cálculo dos "noves fora" de um número pode ser simplificado toda vez que a soma dos algarismos se igualar ou superar 9. Baseados nas proposições 4.7 e 5.4, podemos somar os algarismos do resultado obtido e, assim sucessivamente, até restar um número com apenas um algarismo. Este será os "noves fora" do número inicial.

Exemplo 5.5. 187 "noves fora" 7, significa que o resto da divisão de 187 por 9 é 7. Ou ainda, $187 = 20 \cdot 9 + 7$, ou, equivalentemente, $1 + 8 + 7 = 16$ e $1 + 6 = 7$.

Agora, veremos como se aplica a prova dos noves para as quatro operações básicas: adição, subtração, multiplicação e divisão. A prova dos noves é sustentada pelos resultados a seguir e baseados em [3].

Teorema 5.6 (Propriedade da soma.)**.** *Sejam $a_1, a_2, \ldots, a_n, S \in \mathbb{Z}$. Se $a_1 + a_2 + \ldots + a_n = S$, então o resto da divisão de S por m é igual ao resto da divisão por m da soma dos restos da divisão por m de cada uma das parcelas.*

Demonstração. Seja $S = a_1 + a_2 + \ldots + a_n$. Chamemos de r_s o resto da divisão por m de S e $r_1, \ldots, r_n$, o resto da divisão de $a_1, \ldots, a_n$ por m, respectivamente, onde $0 \leq r_s, r_1, \ldots, r_n < m$. Assim, pelo algoritmo da divisão, existem únicos inteiros $q_1, \ldots, q_n, q_s$ e $0 \leq r_s, r_1, \ldots, r_n < m$ tais que

$$
\begin{aligned}
&a_1 = mq_1 + r_1 \\
&a_2 = mq_2 + r_2 \\
&\vdots \\
&a_n = mq_n + r_n \\
&S = mq_s + r_s.
\end{aligned}
$$

Como, $a_1 + a_2 + \ldots + a_n = S$, temos que

$mq_1 + r_1 + mq_2 + r_2 + \ldots + mq_n + r_n = mq_s + r_s \Leftrightarrow$

$m(q_1 + q_2 + \ldots + q_n) + (r_1 + r_2 + \ldots + r_n) = mq_s + r_s$ (*).

Agora, dividindo $(r_1 + r_2 + \ldots + r_n)$ por m, temos que $(r_1 + r_2 + \ldots + r_n) = mq' + r_k$, onde $0 \leq r_k < m$ e substituindo em (*),

$m(q_1 + q_2 + \ldots + q_n) + mq' + r_k = mq_s + r_s \Leftrightarrow$

$m(q_1 + q_2 + \ldots + q_n + q') + r_k = mq_s + r_s$.

Pelo Algoritmo da Divisão, q_i e r_i são únicos, da última igualdade, temos $r_s = r_k$, onde r_k é o resto da divisão por m da soma dos restos da divisão por m de cada uma das parcelas.

■

Agora, utilizando a notação de congruência e suas propriedades, é possível demonstrar a propriedade da soma de maneira análoga, como veremos a seguir.

Teorema 5.7 (Propriedade da soma)**.** *Sejam $a_1, a_2, \ldots, a_n, S \in \mathbb{Z}$ e $m \in \mathbb{Z}$, $m > 1$. Se $a_1 + a_2 + \ldots + a_n = S$, então $r_1 + r_2 + \ldots + r_n \equiv S (mod\ m)$, onde $r_1, \ldots, r_n$ são os restos da divisão de $a_1, \ldots, a_n$ por m, respectivamente.*

Demonstração. Sejam $S = a_1 + a_2 + \ldots + a_n$ e $r_1, \ldots, r_n$ os restos da divisão de $a_1, \ldots, a_n$ por m, respectivamente, então, por (4.4),

$r_1 \equiv a_1 \pmod{m}$

$r_2 \equiv a_2 \pmod{m}$

$\vdots$

$r_n \equiv a_n \pmod{m}$.

Pelo Teorema 4.5,

$r_1 + r_2 + \ldots + r_n \equiv a_1 + a_2 + \ldots + a_n \pmod{m}$ e

$r_1 + r_2 + \ldots + r_n \equiv S \pmod{m}$,

provam o teorema.

■

Agora, como consequência do Teorema 5.6, temos o seguinte corolário.

Corolário 5.8. *Se $a_1 + a_2 + \ldots + a_n = S$, então o resto da divisão de S por 9 é igual ao resto da divisão por 9 da soma dos restos da divisão por 9 de cada uma das parcelas da soma.*

Demonstração. A demonstração é análoga à prova do Teorema 5.6, basta fazer a substituição de m por 9.

■

A seguir, temos a propriedade da multiplicação.

Teorema 5.9 (Propriedade da multiplicação.)**.** *Sejam $a_1, a_2, \ldots, a_n, P \in \mathbb{Z}$. Se $a_1 a_2 \ldots a_n = P$, então o resto da divisão de P por m é igual ao resto da divisão por m do produto dos restos da divisão por m de cada um dos fatores do produto.*

Demonstração. Seja $P = a_1 \cdot a_2 \cdot \ldots \cdot a_n$. Chamemos de r_p o resto da divisão por P de m e $r_1, \ldots, r_n$, o resto da divisão de $a_1, \ldots, a_n$ por m, respectivamente, onde $0 \leq r_p, r_1, \ldots, r_n < m$. Pelo Algoritmo da Divisão que existem únicos inteiros $q_1, \ldots, q_n, q_p$ e $0 \leq r_p, r_1, \ldots, r_n < m$ tais que

$$\begin{aligned} a_1 &= mq_1 + r_1 \\ a_2 &= mq_2 + r_2 \\ &\vdots \\ a_n &= mq_n + r_n \\ P &= mq_p + r_p. \end{aligned}$$

Como, $a_1 \cdot a_2 \cdot \ldots \cdot a_n = P$, temos que

$(mq_1 + r_1) \cdot (mq_2 + r_2) \cdot \ldots (mq_n + r_n) = mq_p + r_p$, e

$m(q') + (r_1 \cdot r_2 \cdot \ldots \cdot r_n) = mq_p + r_p$ (*) .

Agora, dividindo $(r_1 \cdot r_2 \cdot \ldots \cdot r_n)$ por m, temos que $(r_1 \cdot r_2 \cdot \ldots \cdot r_n) = mq'' + r_k$, onde $0 \leq r_k < m$ e, substituindo em (*),

$m(q') + mq'' + r_k = mq_p + r_p$ e $m(q' + q'') + r_k = mq_p + r_p$.

Pelo Algoritmo da Divisão q_i e r_i são únicos, da última igualdade, temos $r_p = r_k$, onde r_k é o resto da divisão por m do produto dos restos da divisão por m de cada um dos fatores.

■

Da mesma forma, utilizando a notação de congruência e suas propriedades, é possível demonstrar a propriedade da multiplicação de maneira análoga, como a seguir.

Teorema 5.10 (Propriedade da multiplicação.)**.** *Seja* $m \in \mathbb{Z}$*,* $m > 1$*. Se* $a_1 \cdot a_2 \cdot \ldots \cdot a_n = P$*, então* $r_1 \cdot r_2 \cdot \ldots \cdot r_n \equiv P \ (\ mod\ m)$*, onde* $r_1, \ldots, r_n$ *são os restos da divisão de* $a_1, \ldots, a_n$ *por* m*.*

Demonstração. Sejam $r_1, \ldots, r_n, r_p$ o resto da divisão por m de $a_1, \ldots, a_n, P$, respectivamente. Então, por (4.4), temos

$r_1 \equiv a_1 \pmod{m}$

$r_2 \equiv a_2 \pmod{m}$

$\vdots$

$r_n \equiv a_n \pmod{m}$.

Pelo Teorema 4.5, temos

$r_1 \cdot r_2 \cdot \ldots \cdot r_n \equiv a_1 \cdot a_2 \cdot \ldots \cdot a_n \pmod{m}$

$r_1 \cdot r_2 \cdot \ldots \cdot r_n \equiv S \pmod{m}$,

provam o teorema.

■

Como consequência do teorema 5.9 temos o seguinte corolário.

Corolário 5.11. *Sejam* $a_1, a_2, \ldots, a_n, S \in \mathbb{Z}$*. Se* $a_1 a_2 \ldots a_n = P$*, então o resto da divisão de* P *por* 9 *é igual ao resto da divisão do produto dos restos da divisão por* 9 *de cada um dos fatores.*

Demonstração. A demonstração é análoga à prova do Teorema 5.9, basta substituir m por 9.

■

A partir da demonstração das propriedades das soma e multiplicação acima, e também dos Corolários 5.8 e 5.11, podemos apresentar a prova dos noves para as quatro operações: adição, subtração, produto e divisão.

Prova dos noves para adição: Pela propriedade da soma, Teorema 5.6, uma soma *provavelmente* está correta se os “noves fora” da soma, dos “noves fora” das parcelas forem iguais aos “noves fora”do resultado da operação. Isto é, para verificar o resultado de uma soma por meio da prova dos noves, primeiramente tiramos os “noves fora” de cada parcela e somamos. Em seguida, tiramos os “noves fora” desta soma. Os “noves fora” desta soma deve coincidir com os “noves fora” do resultado da operação. Se eles coincidirem, a soma *provavelmente* está correta.

Exemplo 5.12. Vamos aplicar a prova dos noves na operação $345 + 521 = 866$.

Solução. Notemos que,

“Noves fora” da primeira parcela da soma: 345 “noves fora” 3, pois 3+4+5=12 e 1+2=3.

“Noves fora” da segunda parcela da soma: 521 “noves fora”8, pois 5+2+1=8.

Soma do “noves fora” das parcelas: 3+8=11.

“Noves fora” dessa soma (se possível): 1+1=2

“Noves fora” do resultado: $8 + 6 + 6 = 20$ e 2+0=2.

Os “noves fora” do resultado é dado por: 866 “noves fora”2.

Como os “noves fora” da soma dos “noves fora” das parcelas da soma é igual aos “noves fora” do resultado, concluímos que, *provavelmente*, a operação foi realizada corretamente.

Exemplo 5.13. Vamos aplicar a prova dos noves na operação $483 + 628 = 1101$.

Solução. Notemos que,

“Noves fora” da primeira parcela da soma: 483 “noves fora”6, pois 4+8+3=15 e 1+5=6.

“Noves fora” da segunda parcela da soma: 628 “noves fora”7, pois 6+2+8=16 e 1+6=7.

Soma dos “noves fora” das parcelas: 6+7=13.

“Noves fora” dessa soma (se possível): 1+3=4.

“Noves fora” do resultado: $1 + 1 + 0 + 1 = 3$.

Como os “noves fora” da soma dos “noves fora” das parcelas da soma é diferente dos “noves fora” do resultado, concluímos que *certamente* a operação não foi realizada corretamente.

Prova dos noves para subtração: Para aplicarmos a prova dos noves em um subtração, podemos trabalhar com uma soma, pois $x - y = z \Leftrightarrow x = z + y$. Assim, os “noves fora” da soma, dos “noves fora” do resultado da subtração e do subtraendo é igual aos “noves fora” do minuendo. Isto é, para verificar se o resultado de uma subtração está correto, calculamos os "noves fora" do subtraendo e do resultado da subtração e somamos. Em seguida, calculamos os "noves fora" dessa soma. Esse valor deve coincidir com os "noves fora" do minuendo.

Exemplo 5.14. Vamos aplicar a prova dos nove na operação: $93 - 15 = 78$.

Solução.

"Noves fora" do resultado: 78 "noves fora" 6, pois 7+8=15 e 1+5=6.

"Noves fora" do subtraendo: 15 "noves fora"6, pois 1+5=6.

Soma dos "noves fora" do resultado e do subtraendo: 6+6=12.

"Noves fora" dessa soma (se possível): 1+2=3.

"Noves fora" do minuendo: 93 "noves fora"3, pois 9+3=12 e 1+2=3.

Como os "noves fora" da soma, dos "noves fora" do resultado e do subtraendo é igual aos "noves fora" do minuendo, concluímos que, *provavelmente*, a operação foi realizada corretamente.

Exemplo 5.15. Vamos aplicar a prova dos nove na operação: $1768 - 986 = 882$.

Solução.

"Noves fora" do resultado: 882 "noves fora" 0, pois 8 + 8+ 2 = 18 e 1 + 8 = 9.

"Noves fora" do subtraendo: 986 "noves fora"5, pois 9 + 8+ 6 = 23 e 2 + 3 = 5.

Soma dos "noves fora" do resultado e do subtraendo: 0 + 5 = 5.

"Noves fora" do minuendo: 1768 "noves fora"4, pois 1 + 7+ 6 + 8 = 22 e 2 + 2 = 4.

Como os "noves fora" da soma, dos "noves fora" do resultado e do subtraendo é diferente dos "noves fora" do minuendo, concluímos que, *certamente*, a operação está errada.

Prova dos noves para multiplicação: Para aplicar a prova dos noves em uma multiplicação, utilizamos a propriedade da multiplicação, Teorema 5.9, a qual os "noves fora" do produto, dos "noves fora" dos fatores deve ser igual aos "noves fora" do resultado. Isto é, para verificar se o resultado de uma multiplicação está correto, calculamos os "noves fora" de cada fator e multiplicamos. Em seguida, calculamos os "noves fora" deste produto. Se esse último valor coincidir com os “noves fora” do resultado, a operação *provavelmente* estará correta.

Exemplo 5.16. Vamos aplicar a prova dos noves na operação $51 \cdot 26 = 1326$.

Solução. Observemos que,

“Noves fora” do primeiro fator da multiplicação: 51 “noves fora” 6, pois 5+1=6.

“Noves fora” do segundo fator da multiplicação: 26 “noves fora”8, pois 2+6=8.

Produto dos “noves fora” dos fatores: $6 \cdot 8 = 48$.

“Noves fora” do produto dos “noves fora” dos fatores: 48“noves fora”3, pois 4+8=12 e 1+2=3.

*“Noves fora” do resultado da multiplicação:*1326 “noves fora”3, pois 1+3+2+6=12 e 1+2=3.

Como os “noves fora” do produto dos “noves fora” dos fatores é igual aos “noves fora” do resultado, concluímos que, *provavelmente*, a operação foi realizada corretamente.

Exemplo 5.17. Vamos aplicar a prova dos noves na operação $3507 \cdot 29 = 97703$.

Solução. Observemos que,

“Noves fora” do primeiro fator da multiplicação: 3507 “noves fora” 6, pois $3 + 5 + 0 + 7 = 15$ e $1 + 5 = 6$.

“Noves fora” do segundo fator da multiplicação: 29 “noves fora”2, pois $2 + 9 = 11$ e $1 + 1 = 2$.

Produto dos “noves fora” dos fatores: $6 \cdot 2 = 12$.

“Noves fora” do produto dos “noves fora” dos fatores: 12“noves fora”3, pois $1 + 2 = 3$.

*“Noves fora” do resultado da multiplicação:*97703 “noves fora”8, pois $9 + 7 + 7 + 0 + 3 = 17$ e $1 + 7 = 8$.

Como os “noves fora” do produto dos “noves fora” dos fatores é diferente do “noves fora” do resultado, concluímos que, *certamente*, a operação está errada.

Prova dos noves para divisão Para aplicar a prova dos noves na divisão, reescrevemos, a operação como o algoritmo da divisão, isto é, dada uma divisão $\frac{n}{m} = q$ com resto r, onde

$n, m \in \mathbb{Z}, n \neq 0$, podemos escrever $n = mq + r$. Assim, como base nos Teoremas 5.6 e 5.9, os "noves fora", do produto dos "noves fora" do quociente e do divisor somado com o "noves fora" do resto é igual ao "noves fora" do dividendo. Isto é, calculamos os "noves fora" do divisor m e do quociente q. Multiplicamos estes valores e tiramos os "noves fora" quando possível. Em seguida, somamos este resultado com os "noves fora" do resto r, e tiramos os "noves fora" desta soma (quando possível). Este último resultado deve coincidir com os "noves fora" do dividendo n.

Exemplo 5.18. Vamos aplicar a prova dos noves na operação. $2358 \div 17 = 138$ com resto 12.

Solução. Pelo algoritmo da divisão, $2358 = 17 \cdot 138 + 12$. Vamos, então, "conferir" o resultado aplicando a prova dos noves nesta operação. Notemos que

"Noves fora" do divisor: 17 "noves fora" 8, pois 1+7=8.

"Noves fora" do quociente: 138 "noves fora"3, pois 1+3+8=12 e 1+2=3.

"Noves fora" do produto dos "noves fora" do quociente e do divisor: $8 \cdot 3 = 24$. Assim, temos 24 " "6, pois 2+4=6.

"Noves fora" do resto: 12 "noves fora"3, pois 1+2= 3.

"Noves fora" da soma, dos "noves fora" do resto com os "noves fora" do produto dos "noves fora" do quociente e do divisor: 6+3=9, logo, 9 "noves fora" 0.

"Noves fora" do dividendo: 2358 "noves fora"0, pois 2+3+5+8=18 e 1+8=9.

Assim, concluímos que, *provavelmente*, a operação foi realizada corretamente.

Exemplo 5.19. Vamos aplicar a prova dos noves na operação. $593 \div 83 = 7$ com resto 22.

Solução. Pelo algoritmo da divisão, temos que $593 = 83 \cdot 7 + 22$. Vamos então "conferir" aplicando a prova dos noves nesta operação.

"Noves fora" do divisor: 83 "noves fora" 2, pois $8 + 3 = 11$ e $1 + 1 = 2$.

"Noves fora" do quociente: 7 "noves fora"7.

"Noves fora" do produto dos "noves fora" do quociente e do divisor: $2 \cdot 7 = 14$. Assim, temos 14 "noves fora "5, pois $1 + 4 = 5$.

"Noves fora" do resto: 22 "noves fora"4, pois $2 + 2 = 4$.

"Noves fora" da soma, dos "noves fora" do resto com os "noves fora" do produto dos "noves fora" do quociente e do divisor: $4 + 5 = 9$, logo, 9 "noves fora" 0.

"Noves fora" do dividendo: 593 "noves fora"8, pois $5 + 9 + 3 = 17$ e $1 + 7 = 8$.

Assim, concluímos que, *certamente*, a operação está errada.

Logo, observamos que o que a prova dos noves faz, é substituir a operação $a_1 + a_2$ por $r_1 + r_2$, por exemplo, e verificar se quando são divididos por 9, deixam o mesmo resto que o resultado da operação matemática, quando também é dividido por 9. Isso torna a prova dos noves um processo prático, pois não há grande dificuldade em determinar r_1 e r_2 e torna maior a chance de que o erro esteja na operação matemática, e não na prova dos noves.

Capítulo 6

A Prova dos noves como condição necessária

Neste capítulo veremos que a prova dos noves é uma condição necessária, mas não é suficiente para afirmar se determinada operação matemática foi realizada corretamente. Veremos o porquê e em quais casos isso acontece. Também falaremos sobre o motivo da prova utilizar o resto de uma divisão por 9 e não por outro número inteiro positivo, ou seja, porque não fazer a prova dos setes ou a prova dos onze, por exemplo.

6.1 Quando a Prova dos Noves falha?

Vimos que a prova dos noves é um método de verificação para operações matemáticas básicas. E de fato, se uma operação matemática for realizada corretamente e a prova dos noves também for realizada corretamente, esta sempre irá confirmar a exatidão dessa resposta. Agora, se a operação matemática não for realizada corretamente, a prova dos noves nem sempre acusará o erro. Em outras palavras, a prova dos noves pode falhar, e a possibilidade de falha ocorre quando a operação matemática não for realizada corretamente. Portanto, a prova dos noves é uma condição necessária e não suficiente.

Isto é, sejam p: operação realizada corretamente e q: prova dos noves indicando que o resultado da operação matemática está correto, as proposições a serem analisadas. É importante ressaltar que estamos assumindo que a prova dos noves foi realizada corretamente.

Com isso, temos que $p \to q$, isto é, se a operação matemática foi realizada corretamente, então a prova dos noves vai acusar que este resultado está correto. Isso é equivalente a

$\sim q \to \sim p$, isto é, se a prova dos noves indicou erro na operação, então esta operação não foi realizada corretamente.

Mas, usando lógica, temos que se p é falsa, ela implica tanto em q falsa como em q verdadeiro. Em outras palavras, se a operação não foi realizada corretamente, então a prova dos noves pode acusar ou não o erro.

A prova dos noves não conseguirá identificar o erro quando o resultado obtido de forma errada e o resultado que seria correto deixam mesmos restos quando divididos por 9, isto é, os "noves fora" de ambos são iguais.

Ou, equivalentemente, todas as vezes em que a diferença entre o resultado correto e o resultado calculado de forma errada for um múltiplo de 9, a prova dos noves vai falhar, isto é, ela acusará que a operação foi realizada corretamente, quando de fato, está errada. Vamos agora demonstrar este resultado.

Proposição 6.1. *Sejam n e n' números naturais. A diferença $n - n'$ é um múltiplo de 9 se, e somente se, n e n' deixam mesmos restos quando dividos por 9.*

Demonstração: Sejam n e n' números naturais. Pelo algoritmo da divisão, existem únicos q, q', r, r' com $0 \leq r, r' < 9$ inteiros, tais que $n = 9q + r$ e $n' = 9q' + r'$.

Temos de $r = r'$ que $r - r' = 0$. Assim, $n - n' = 9(q - q')$. Logo, $9 | n - n'$, isto é, $n - n'$ é um múltiplo de 9.

■

Vejamos alguns exemplos:

Exemplo 6.2. Suponhamos que ao efetuar a operação $23 \cdot 15$, obtemos 354, quando o resultado correto seria 345.

Solução. Observemos que a diferença entre os resultados correto e incorreto, 354 - 345 = 9, é múltiplo de 9, e pela Proposição 6.1, ambos deixam mesmo restos quando divididos por 9.

Se ambos deixam mesmos restos, a prova dos noves não vai identificar o erro.

Vamos verificar aplicando a prova dos noves nesta operação:
23 "noves fora" 5, 15 "noves fora" 6 e 354 "noves fora"3.

Como o produto dos "noves fora" dos fatores é 30 "noves fora" 3, coincide com os "noves fora" de 354, temos que a prova dos noves está acusando que a conta está correta, quando na realidade não está.

Observemos que, além dos resultados correto e incorreto, deixarem mesmo resto quando divididos por 9, como os algarismos de ambos valores (o errado e o correto) são iguais, a soma será igual e o resto da divisão dessa soma por 9 também será a mesma, isto ocorre porque a prova dos noves consiste na soma dos algarismos.

Logo, um caso particular em que a prova dos noves não identifica o erro, ocorre quando os resultados (errado e correto) possuem os mesmos algarismos, e se diferem apenas pela posição ocupada de cada algarismo.

Exemplo 6.3. Suponhamos que ao efetuar a operação $786 + 127$, obtemos 904, quando o resultado correto seria 913.

Solução. Observemos que a diferença entre os resultados correto e incorreto, 913 - 904 = 9, é múltiplo de 9, e pela Proposição 6.1, ambos deixam mesmo restos quando divididos por 9.

Se ambos deixam mesmos restos, a prova dos noves não vai identificar o erro.

Vamos verificar aplicando a prova dos noves nesta operação:
786 "noves fora" 3, 127 "noves fora" 1 e 904 "noves fora" 4.

Como os "noves fora" da soma dos "noves fora" das parcelas da soma é igual aos "noves fora" do resultado, a prova dos noves está acusando que a conta está correta, quando na realidade não está.

Se a prova dos noves pode falhar, torna-se relevante fazer algumas estimativas da porcentagem de casos em que ela falha ao ser aplicada em uma operação.

6.2 Estimativa de erro

Nesta seção, iremos calcular algumas estimativas de erros e determinar sua porcentagem de falha para alguns casos particulares de aplicação da prova dos noves. Para isso, suponhamos que uma operação matemática foi realizada e vamos estabelecer a condição de que a prova dos noves foi executada corretamente nesta operação matemática. Temos, então, dois casos a considerar:

1. Se ao executar a prova dos noves, os restos da divisão por nove do resultado e da soma dos restos da divisão por 9 das parcelas da operação forem diferentes, com certeza, a prova identificou o erro;

2. Se, ao executar a prova dos noves, os restos da divisão por nove do resultado da operação e da soma dos restos da divisão por 9 das parcelas forem iguais, pode ser que a prova não tenha identificado o erro.

Então, há quantas possibilidades de falso positivo, isto é, quantos são os resultados errados possíveis que a prova dos noves não identifica?

Temos, no item 1., os casos em que a prova dos noves não apresenta falha. Logo, vamos nos ater em responder, ao menos parcialmente, a pergunta baseada no caso apresentado no item 2.

Primeiramente, sabemos que a prova dos noves falhará quando o resto da divisão por 9 do resultado da operação coincidir com o resto da divisão por 9 do resultado correto. Vamos apresentar alguns casos particulares e calcular a porcentagem de falha para cada um dos casos. Para isso, vamos nos ater ao caso de uma operação de adição com números naturais. Para as demais operações básicas (subtração, multiplicação e divisão), procederíamos de forma análoga, pois o objetivo é fazer a análise do resultado da operação matemática realizada.

A ideia é contabilizar quantos resultados possíveis (errados) de uma operação matemática, deixam o mesmo resto quando dividos por 9 que o resultado correto, e calcular a porcentagem em relação aos casos possíveis.

Para isso, inicialmente, elaboramos uma tabela que apresenta a quantidade de números com 2, 3, 4 e 5 algarismos que deixam resto 0, 1, 2, 3, 4, 5, 6, 7 e 8 quando divididos por 9.

N. de algarismos	*Quantidade de números que deixam resto:*								
	0	1	2	3	4	5	6	7	8
2	12	11	11	11	11	11	11	11	11
3	112	111	111	111	111	111	111	111	111
4	1112	1111	1111	1111	1111	1111	1111	1111	1111
5	11112	11111	11111	11111	11111	11111	11111	11111	11111

Tabela 6.1: Quantidade de números com 2, 3, 4 e 5 algarismos que deixam resto 0, 1, 2, 3, 4, 5, 6, 7 e 8 quando divididos por 9.

Essa tabela foi elaborada por meio de uma contagem simples realizada em uma planilha de cálculo.

Exemplo 6.4. Consideremos a operação matemática,

$$a_1a_2 + b_1b_2 = c_1c_2,$$

onde $a_1, a_2, b_1, b_2, c_1, c_2$, são os algarismos dos números que compõem a operação matemática. Vamos calcular, qual a porcentagem de falha da prova dos noves em identificar que este resultado está errado.

Solução. Observemos que o resultado c_1c_2 possui dois algarismos. Podemos supor que existem $10^2 = 100$ números distintos de 2 algarismos, para efeito de simplificação. Observemos que aqui estamos considerando que $01, 02, \ldots, 09$ possuem dois algarismos. Estes são todos os resultados possíveis de ocorrer.

Pela Tabela 6.1, temos 12 números de dois algarismos se o resultado da operação deixa resto 0 quando divido por 9, e temos 11 números de dois algarismos, se o resultado da operação deixa resto 1, 2, 3, 4, 5, 6, 7 ou 8, quando divido por 9.

Então, temos dois casos:

1. O resultado deixa resto 0.

2. O resultado deixa resto 1, 2, 3, 4, 5, 6, 7 ou 8.

No caso do item 1., temos que existem 12 números que deixam resto 0 quando divididos por 9. Um deles é o correto. Logo, há 11 números possíveis que podem aparecer e que a prova não identifica o erro, em 100 resultados possíveis, o que nos fornece uma porcentagem de $\dfrac{11}{100} = 0,11$, isto é 11%.

Agora, no caso do item 2., temos que existem 11 números que deixam resto 1, 2, 3, 4, 5, 6, 7 ou 8 quando divididos por 9. Um deles é o correto. Logo, há 10 números possíveis que podem aparecer e a prova não identifica o erro, em 100 resultados possíveis, o que nos fornece uma porcentagem de $\dfrac{10}{100} = 0,10$, isto é 10%.

Logo, no pior dos casos, teremos 11% de chance da prova dos noves falhar.

Exemplo 6.5. Consideremos a operação matemática realizada

$$a_1a_2a_3 + b_1b_2 = c_1c_2c_3,$$

onde $a_1, a_2, a_3, b_1, b_2, c_1, c_2, c_3$ são os algarismos dos números que compõem a operação matemática. Vamos calcular, qual a porcentagem de falha da prova dos noves em identificar que este resultado está errado.

Solução. Observemos que o resultado $c_1c_2c_3$ possui três algarismos. Podemos supor que existem $10^3 = 1000$ números distintos de três algarismos, para efeito de simplificação. Observemos que aqui estamos considerando que $01, 02, \ldots, 099$ possuem três algarismos. Estes são todos os resultados possíveis de ocorrer.

Então, temos dois casos a analisar:

1. O resultado da operação matemática realizada deixou resto 0.

2. O resultado deixou resto 1, 2, 3, 4, 5, 6, 7 ou 8.

No caso do item 1., pela Tabela 6.1, temos que existem 112 números que deixam resto 0 quando divididos por 9. Um deles é o correto. Logo, há 111 números possíveis que podem aparecer e que a prova não identifica o erro, em 1000 resultados possíveis, o que nos fornece uma porcentagem de $\dfrac{111}{1000} = 0,111$, isto é $11,1\%$.

Agora, no caso do item 2., pela Tabela 6.1, temos que existem 111 números que deixam resto 1, 2, 3, 4, 5, 6, 7 ou 8 quando divididos por 9. Um deles é o correto. Logo, há 110 números possíveis que podem aparecer e a prova não identifica o erro, em 1000 resultados possíveis, o que nos fornece uma porcentagem de $\dfrac{110}{1000} = 0,11$, isto é 11%.

Logo, no pior dos casos, teremos $11,1\%$ de chance da prova dos noves falhar.

Exemplo 6.6. Consideremos a operação matemática,

$$a_1a_2a_3a_4 + b_1b_2b_3 = c_1c_2c_3c_4,$$

onde $a_1, a_2, a_3, a_4, b_1, b_2, b_3, c_1, c_2, c_3, c_4$ são os algarismos dos números que compõem a operação matemática. Vamos calcular, qual a porcentagem de falha da prova dos noves em identificar que este resultado está errado.

Solução. Observemos que o resultado da operação, $c_1c_2c_3c_4$, possui quatro algarismos. Podemos supor que existem $10^4 = 10000$ números distintos de quatro algarismos, para efeito de simplificação. Observemos que aqui estamos considerando que $01, 02, \ldots, 0999$ possuem quatro algarismos. Estes são todos os resultados possíveis de ocorrer.

Então, temos dois casos a analisar:

1. O resultado da operação matemática realizada deixou resto 0.

2. O resultado deixou resto 1, 2, 3, 4, 5, 6, 7 ou 8.

No caso do item 1., pela Tabela 6.1, temos que existem 1112 números que deixam resto 0 quando divididos por 9. Um deles é o correto. Logo, há 1111 números possíveis que podem aparecer e a prova não identifica o erro, em 10000 resultados possíveis, o que nos fornece uma porcentagem de $\dfrac{1111}{10000} = 0,1111$, isto é $11,11\%$.

Agora, no caso do item 2., temos que existem 1111 números que deixam resto 1, 2, 3, 4, 5, 6, 7 ou 8 quando divididos por 9. Um deles é o correto. Logo, há 1110 números possíveis que podem aparecer e a prova não identifica o erro, em 10000 resultados possíveis, o que nos fornece uma porcentagem de $\dfrac{1110}{10000} = 0,111$, isto é $11,10\%$.

Logo, no pior dos casos, teremos $11,11\%$ de chance da prova dos noves falhar.

Exemplo 6.7. Consideremos a operação matemática,

$$a_1a_2a_3a_4a_5 + b_1b_2b_3b_4b_5 = c_1c_2c_3c_4c_5,$$

onde $a_1, a_2, a_3, a_4, a_5, b_1, b_2, b_3, b_4, b_5, c_1, c_2, c_3, c_4, c_5$ são os algarismos dos números que compõem a operação. Vamos calcular, qual a porcentagem de falha da prova dos noves em identificar que este resultado está errado.

Solução. Observe que o resultado $c_1c_2c_3c_4c_5$ possui cinco algarismos. Podemos supor que existem $10^5 = 100000$ números distintos de cinco algarismos, para efeito de simplificação. Observemos que estamos considerando que $01, 02, \ldots, 09999$ possuem cinco algarismos. Estes são todos os resultados possíveis de ocorrer.

Então, temos dois casos a analisar:

1. O resultado da operação matemática realizada deixou resto 0.

2. O resultado deixou resto 1, 2, 3, 4, 5, 6, 7 ou 8.

No caso do item 1., pela Tabela 6.1, temos que existem 11112 números que deixam resto 0 quando divididos por 9. Um deles é o correto. Logo, há 11112-1=11111 números possíveis que podem aparecer e a prova não identifica o erro, em 100000 resultados possíveis, o que nos fornece uma porcentagem de $\dfrac{11111}{100000} = 0,11111$, isto é $11,111\%$.

Agora, no caso do item 2., temos que existem 11111 números que deixam resto 1, 2, 3, 4, 5, 6, 7 ou 8 quando divididos por 9. Um deles é o correto. Logo, há 11111 - 1 = 11110 números possíveis que podem aparecer e que a prova não identifica o erro, em 100000 resultados possíveis, o que nos fornece uma porcentagem de $\dfrac{11110}{100000} = 0,1111$, isto é $11,11\%$.

Logo, no pior dos casos, teremos $11,111\%$ de chance da prova dos noves falhar.

Podemos identificar padrões nos exemplos apresentados, e com isso, podemos intuir que a porcentagem de ocorrer falha ao aplicar a prova dos noves, dependendo da quantidade de algarismos do resultado da operação matemática realizada, varia em um teto máximo de 12%.

Agora, vamos analisar alguns casos específicos de erros que podem ocorrer ao realizar operações matemáticas e determinar a porcentagem de falha da prova dos noves para estes casos. Vejamos, então, alguns exemplos específicos:

Exemplo 6.8. Suponhamos que efetuamos a operação $79 + 89 = 158$, quando o resultado correto seria 168.

Podemos observar que o resultado está errado em uma dezena, e como a diferença entre o resultado correto e o obtido é $168 - 158 = 10$ que não é múltiplo de nove (Proposição 6.1), a prova dos noves não vai falhar, isto é, ela vai identificar o erro.

Exemplo 6.9. Suponhamos que ao efetuamos a operação $79+89 = 157$, quando o resultado correto seria 168.

Podemos observar que o resultado está errado em uma unidade, e como a diferença entre o resultado correto e o obtido é $168 - 157 = 11$ que não é múltiplo de nove (Proposição 6.1), a prova dos noves não vai falhar, isto é, ela vai identificar o erro.

É importante observar que o valor de 12% foi obtido considerando todas os resultados possíveis para determinada operação matemática, e que essa porcentagem de falha pode ser reduzida se retiramos resultados em que há chance mínima ou nenhuma de ocorrer, podendo ser desconsiderados. E que erros comuns de acontecer, como errar em uma unidade ou uma dezena, como apresentado nos exemplos anteriores, são casos em que a prova dos noves identifica o erro, ou seja, ela não falha.

6.3 O porquê da prova ser dos "noves"

Vimos que os Teoremas 5.6 e 5.9 são a base da prova dos noves, e nos enunciados destes teoremas, não existem restrições quanto ao número que usamos para efetuar a divisão das parcelas. Esses resultados valem para um m natural qualquer. Inclusive, apresentamos nos Corolários 5.8 e 5.11, propriedades dos restos, especificamente de uma divisão por 9. Logo, não haveria problema se ao invés de efetuarmos a prova dos noves em uma operação matemática, decidíssimos tirar os três fora, setes fora, onzes fora, entre outros. Essas provas se basearia em determinar o resto da divisão das parcelas por esses valores (três, sete, onze, por exemplo).

O fato é que existem algumas justificativas que tornam a prova dos noves mais prática de ser efetuada do que a prova de outro número m natural qualquer. Vejamos:

1. Calcular o resto da divisão de um número por nove é bem mais prático do que calcular o resto da divisão de um número por sete, por exemplo. Uma boa opção poderia ser

calcular a prova dos três ou onzes, no entanto, temos poucas possibilidades de restos de uma divisão por três, isto é, $\{0, 1, 2\}$ o que aumenta a chance da prova validar uma operação realizada de forma errada. Já a prova dos onzes seria interessante, no entanto, o critério de divisibilidade por 9 é mais prático do que do critério de divisibilidade por 11. Os números 2, 4, 5, 8, 10 e 25 não são uma boa escolha para divisores desta prova, pois não utilizam todos os algarismos dos números, o que não seria conveniente, pois haveria um número maior de vezes em que a prova validaria uma operação matemática realizada de forma incorreta, para mais detalhes veja [3].

2. Outro fator é que a base do nosso sistema de numeração é decimal. Como 10^i deixa resto 1 quando dividido por 9, para todo $i > 0$, isso faz com que o resto da divisão de um número por 9 possa ser determinado calculando a soma desses algarismos por 9 e, em seguida, dividindo-o por 9, ou podemos somar os algarismos do resultado obtido, e, assim sucessivamente, até restar um número com um único algarismo.

Capítulo 7

Considerações finais

Este trabalho apresentou um estudo sobre a prova dos noves e a teoria pela qual a mesma se baseia. Para isso, inicialmente, realizamos uma revisão bibliográfica sobre números inteiros, divisibilidade e congruência para posterior construção das teorias que sustentam a prova dos noves.

Vimos que a prova dos noves é uma regra usada para identificar erros em operações matemáticas básicas e não foram encontradas referências sobre a origem da prova dos noves nem a partir de que época esta foi inserida nos currículos escolares. O que se encontram são indícios que esta regra vem de séculos atrás.

Entretanto, com a popularização do uso das calculadoras, a prova dos noves caiu em desuso e não é mais ensinada nas escolas, o que foi um dos estímulos para realização deste trabalho.

No decorrer do trabalho, vimos que a prova dos noves é uma condição necessária mas não suficiente, e que, ela pode falhar, conforme apresentado e demonstrado anteriormente. Essa questão nos chamou a atenção e nos motivou a calcular e apresentar algumas estimativas de erros, contextualizando, para casos particulares, a porcentagem de falha da prova dos noves, isto é, determinamos qual a probabilidade da prova dos noves não identificar o erro em uma determinada operação matemática, já que não encontramos na bibliografia pesquisada essa abordagem nem relatos sobre a porcentagem de falha da prova dos noves.

De alguns casos particulares, obtivemos valores de falha em um teto máximo de 12%. Logo, ao aplicar a prova dos noves em uma operação matemática, não podemos afirmar que a operação foi realizada corretamente, mas com certeza, o resultado tornou-se mais confiável, pois passou por um teste de verificação.

Na nossa opinião, pensamos que o resgate da prova dos noves, mesmo não sendo necessariamente essencial, seria útil no contexto escolar, pois conceitos como sistemas de numeração e divisibilidade são indispensáveis para sua fundamentação teórica, e segundo as Diretrizes Curriculares Estaduais do Estado do Paraná, o professor pode acrescentar outros conteúdos básicos em sua proposta pedagógica de modo a enriquecer seu trabalho e contribuir para o processo de ensino e aprendizagem da matemática, veja [14].

Acreditamos também que, a inserção da prova dos noves nas propostas pedagógicas, estímula o cálculo escrito e mental, o que ajuda o aluno a organizar o seu pensamento, desenvolver o raciocínio lógico, agiliza o seu trabalho cognitivo, e possibilita ao aluno criar estratégias de resolução, desenvolve a memória e concentração, contribuindo também nas relações sociais deste aluno. Além disso, é possível descobrir conceitos e propriedades inerentes às operações matemáticas [1].

Concluímos que o trabalho atingiu nossos objetivos e abrangeu os temas abordados de maneira esperada ao apresentar uma análise fundamentada sobre a prova dos noves, além de expor algumas estimativas de erros para casos particulares de aplicação da prova dos noves em operações básicas.

Bibliografia

[1] ANANIAS, E. F., *O cálculo mental na educação matemática: aspectos teóricos metodológicos de uma pesquisa de mestrado* In: Anais do XI ENEM – SBEM, Curitiba, PR; julho, 2013. Disponível em: http://sbem.web1471.kinghost.net/anais/XIENEM/pdf/1235_975_ID.pdf. Acesso em 04 de fevereiro de 2018.

[2] BEZERRA, S. *Como Me Tornei Professora De Matemática: Memórias Resgatadas Através Da História Da Educação Matemática.*, In: Anais do XI ENEM – SBEM, Curitiba, PR; julho, 2013. Disponível em: http://sbem.web1471.kinghost.net/anais/XIENEM/pdf/1657_1163_ID.pdf. Acesso em 04 de fevereiro de 2018.

[3] CRUZ, J., Z. da S., *Divisibilidade e prova dos noves*, 53p. Monografia (Licenciatura em Matemática), Universidade Estadual do Oeste do Paraná, Cascavel, 2009.

[4] EVARISTO, J., PERDIGÃO, E., *Introdução à Álgebra Abstrata*, Formato Digital/Versão 01.2013, Maceio, 2013.

[5] EVES, H. *Introdução à História da Matemática*, Trad. Hygino H. Domingues. Campinas, SP. Editora da Unicamp, 2004.

[6] FERREIRA, F. de A., *A Prova dos Noves, Divisibilidade e Congruência*, 53p. Dissertação de mestrado. Universidade Federal do Cariri, Juazeiro do Norte, 2017.

[7] GIMENES, L. P., *Teorema Fundamental da Aritmética*, Disponível em: http://www.dma.uem.br/kit/. Acesso em 02 de abril de 2018.

[8] GONÇALVES, A., *Introdução à Álgebra.*, 5. edição, Rio de Janeiro: IMPA, 2007.

[9] HEFEZ, A., *Aritmética. Coleção PROFMAT*, Rio de Janeiro: SBM, 2014.

[10] LACAVA, A. G. *Um estudo sobre diferentes abordagens da prova dos nove presentes em livros didáticos de aritmética (1890-1970)*, 154p. Dissertação de mestrado. Universidade Federal de Santa Catarina, Florianópolis, 2017.

[11] LACAVA, A. G.; COSTA, D. A. *A prova dos nove e o caso da "Arithmetica Primaria" de Cezar Pinheiro.* REVEMAT, Florianópolis/SC, v.11, n. 1, p. 54-73, 2016. Disponível em: https://periodicos.ufsc.br/index.php/revemat/article/viewFile/1981-1322.2016v11n1p54/32128. Acesso em 12 de janeiro de 2018.

[12] LIMA, A., et al. *A Matemática do Ensino Médio*, volume 2, 6. edição, Rio de Janeiro: Coleção Professor de Matemática. SBM, 2009.

[13] OLIVEIRA, A., LUTOSA, L., *A prova dos nove*, In: Caderno dá licença. Universidade Federal Fluminense. Vol1. Ano 1. Dez/1998. Disponível em: http://www.uff.br/dalicenca/images/stories/caderno/volume1/a_prova_ dos_nove.pdf . Acesso em 30 de agosto de 2017.

[14] PARANÁ, *Diretrizes Curriculares Para a Escola Pública.* Site oficial do Estado do Paraná. Disponível em: www.diaadiaeducacao.pr.gov.br. Acesso em 04 de fevereiro de 2018.

[15] RODRIGUES, F. W., *A Prova dos Noves*, Revista do Professor de Matemática, n. 14. Rio de Janeiro: SBM, 2009. Disponível em: http://rpm.org.br/cdrpm/14/3.htm dos_nove.pdf . Acesso em 07 de novembro de 2017.

[16] SANTOS, J. P. de O., *Introdução à Teoria dos Números.*, 3. edição, Rio de Janeiro: IMPA, 2009.

[17] WATANABE, R. *Na Terra dos Noves-Fora*, Coleção Vivendo a Matemática. 2.edição, Editora Scipione.