ATLANTE
Cuadernos de Educación y Desarrollo (2ª Época)

Febrero 2020 - ISSN: 1989-4155

ARITMÉTICA: UM CAMINHO PARA ADQUIRIR HABILIDADE EM DEMONSTRAÇÕES

ARITHMETIC: A PATH TO GAINING SKILL IN DEMONSTRATIONS

ARITMÉTICA: UN CAMINO PARA ADQUIRIR DESTREZA EN DEMOSTRACIONES

Marcos Garcia de Souza[1]
Samuel Antonio Silva do Rosario[2]

Para citar este artículo puede utilizar el siguiente formato:

Marcos Garcia de Souza y Samuel Antonio Silva do Rosario (2020): "Aritmética: um caminho para adquirir habilidade em demonstrações", Revista Atlante: Cuadernos de Educación y Desarrollo (febrero 2020). En línea:

https://www.eumed.net/rev/atlante/2020/02/aritmetica-habilidade-demonstracoes.html
http://hdl.handle.net/20.500.11763/atlante2002aritmetica-habilidade-demonstracoes

RESUMO

De um modo geral, a estrutura da Matemática está vinculada a teoremas, cuja validade dar-se-á por meio de demonstração. Assim, é necessário que o estudioso da matemática saiba justificar determinadas afirmações. Para isso, é importante adquirir técnicas e habilidades em demonstrações. Nesse sentido, propomos a Aritmética como um meio de aquisição desses procedimentos, pois, nesta disciplina, existem diversas proposições de natureza simples que, gradativamente, tornam-se complexas, possibilitando o amadurecimento de técnicas de demonstrações em Matemática. Neste escrito, há vários exemplos resolvidos e teoremas demonstrados para proporcionar ao leitor experiências em demonstrações de proposições de matemática. Em particular, destacam-se a Propriedade Arquimediana, o Princípio de Indução Matemática, a Divisão Euclidiana e a representação única de um número no Sistema de Numeração Posicional, numa determinada base, como proposições/teoremas mais importantes neste texto. Ressalta-se ainda que propomos uma possibilidade de ensinar a operação de divisão por meio da "Tabuada de Multiplicação". Assim, espera-se que a forma de adquirir habilidade de demonstrações em Matemática seja facilitada, por experiência primeira, partindo-se da Aritmética.

PALAVRAS-CHAVE: Aritmética; Demonstrações Matemáticas; Habilidades Matemáticas; Técnicas Matemáticas.

RESUMEN

En general, la estructura de las matemáticas está vinculada a los teoremas, cuya validez se dará por demostración. Por lo tanto, es necesario justificar ciertas afirmaciones. Para esto es importante

[1] Professor do Instituto Federal do Pará – IFPA (Campus Marabá Industrial), Mestre em Matemática (UFPA), Especialista em Matemática.(UNICAMP), Graduado em Matemática (UNICAMP), E-mail: marcos.souza@ifpa.edu.br
[2] Professor do Instituto Federal do Pará – IFPA (Campus Marabá Industrial), Mestre em Matemática (UFPA), Especialista em Matemática e Ciências Naturais (FCV), Especialista em Ciências Biológicas (FAERPI), Graduado em Matemática (UEPA), Graduado em Ciências Biológicas (UNIASSELVI), E-mail: samuel.rosario@ifpa.edu.br

adquirir habilidades y técnicas de demostración. En este sentido, proponemos la aritmética como un medio para adquirir estos procedimientos, porque en esta disciplina hay varias proposiciones simples que gradualmente se vuelven complejas, permitiendo la maduración de las técnicas de demostración matemática. En este escrito, hay varios ejemplos resueltos y teoremas demostrados para proporcionar al lector experiencias en la demostración de proposiciones matemáticas. En particular, la Propiedad Arquímedeana, el Principio de Inducción Matemática, la División Euclidiana y la representación única de un número en el Sistema de Numeración Posicional, sobre una base dada, se destacan como las proposiciones/teoremas más importantes en este texto. También es digno de mención que proponemos una posibilidad de enseñar la operación de división a través de la "Tabla de Multiplicación". Por lo tanto, se espera que la primera experiencia, a partir de la aritmética, facilite la forma de adquirir habilidades de demostración en matemática.
PALABRAS CLAVE: Aritmética; Demostraciones matemáticas; Habilidades matemáticas; Técnicas Matemáticas.

ABSTRACT

In general, the structure of mathematics is linked to theorems, whose validity will be given by demonstration. Thus, it is necessary that the student of mathematics can justify certain statements. For this it is important to acquire demonstration skills and techniques. In this sense, we propose Arithmetic as a means of acquiring these procedures, because in this discipline, there are several simple propositions that gradually become complex, allowing the maturation of mathematical demonstration techniques. In this writing, there are several solved examples and theorems demonstrated to provide the reader with experiences in demonstrating mathematical propositions. In particular, the Archimedean Property, the Mathematical Induction Principle, the Euclidean Division, and the unique representation of a number in the Positional Numbering System, on a given basis, stand out as the most important propositions/theorems in this text. It is also emphasized that we propose a possibility to teach the division operation through the "Multiplication Table". Thus, it is expected that the way to acquire demonstration skills in mathematic will be facilitated by first experience, starting from arithmetic.
KEYWORDS: Arithmetic; Mathematical demonstrations; Mathematical skills; Mathematical Techniques.

1. INTRODUÇÃO

A Aritmética é uma das ramificações da matemática que possui enorme diversidade em conceitos, que vai do simples ao complexo.

Num nível elementar, a Aritmética apresenta o conceito de divisibilidade por meio da relação "dividir", com a condição do resto ser igual a zero.

A operação de multiplicação é essencial para compreender a operação de divisão com resto. Ela pode ser facilitada utilizando-se a "Tabuada de Multiplicação".

Com isso, enseja-se a possibilidade de adquirir técnicas e habilidades de demonstrações utilizando-se as operações básicas da Matemática (adição, subtração, multiplicação e divisão) e os conceitos elementares de Aritmética.

2. DIVISIBILIDADE

2.1 Múltiplos e Divisores em = {1, 2, 3, ...}

Intrinsecamente, a *divisibilidade* é uma *relação* que expressa a divisão de dois números naturais, com *resto* igual a *zero*.

Nesse sentido, dados dois números naturais a e $b \neq 0$, dizemos que $b \mid a$ (lê-se: "b divide a") se *existir* um número natural c, tal que $a = bc$. Caso contrário, dizemos que b *não* divide a, e escrevemos b a. O número b chama-se *divisor* (ou *fator*) do número a. O número a chama-se *múltiplo* de b e indica-se por $a = mb$.

Observações:

1) A notação $b \mid a$ (b divide a) não é uma operação em , muito menos uma fração. Ela representa, precisamente, uma *relação de divisibilidade* de a por b, com *resto zero*;

2) Daqui por diante, o conjunto dos números naturais com zero será indicado por $_0$ = $\cup \{0\} = \{0, 1, 2, 3, ...\}$;

3) Se $b \mid a$, sabemos que existe um $c \in$, tal que $bc = a$. Nesta equação, o número c, que indicaremos por $c =$, chama-se *quociente* de a por b.

Existe uma semelhança entre a *relação de divisibilidade* e a *relação de ordem* em , a saber:

Relação *divide*: $b \mid a$ $c \in$; $a = bc$.

Relação de *limitação*: $b \leq a$ $c \in$; $a = b + c$.

Nesse sentido, a divisibilidade é *multiplicativa* e a relação de ordem é *aditiva*, ambas em . A partir disso, é possível estabelecer diversas propriedades, cujas demonstrações baseiam-se em conceitos que têm essas características. Destaca-se, ainda, que não vale a propriedade da tricotomia para a relação de divisibilidade. Por exemplo, não vale a propriedade reflexiva, de fato: 1 divide 2, mas 2 não divide 1.

A relação de divisibilidade possibilita elaborar algumas proposições.

Proposição 1. Sejam $a, b, c \in$, com $a, b \neq 0$. Então:

i) $a \mid 0$; $a \mid a$ e $1 \mid a$.

ii) $a \mid 1$ se, e somente se, $a = 1$.

iii) $a \mid b$ e $a \mid c$ implicam $a \mid (bx \pm cy)$, para todo $x, y \in$. Neste caso, o termo $(bx \pm cy)$ chama-se *combinação linear* de b e c.

iv) $a \mid b + c$ e $a \mid b$ implicam $a \mid c$.

v) $a \mid b$ e $b \mid c$ implicam $a \mid c$ (*propriedade transitiva*)

Demonstração: **i)** $0 = 0.a$ implica $a \mid 0$; $a = 1.a$ implica $a \mid a$ e $1 \mid a$.

ii) $a \mid 1$ implica $1 = am$, para algum $m \in$. Se $m = 1$, então, $a = 1$.

Agora, se $m \neq 1$, então $m > 1$ implica $am > m$ e, portanto, $1 > a$, o que é um absurdo! Logo, $a = 1$.

iii) $a \mid b$ e $a \mid c$ implicam $b = ma$ e $c = na$, onde $m, n \in$ e, portanto, $bx = max$ e $cy = nay$, onde $x, y \in$.

Somando (ou subtraindo) os membros dessas igualdades, temos:

$$bx \pm cy = max \pm nay = (mx \pm ny)a = ka, \text{ para algum } k \in .$$

Portanto, $a \mid bx \pm cy$.

iv) $a \mid b + c$ e $a \mid b$ implicam $b + c = ma$ ou $c = ma - b$ e $b = na$, para $m, n \in$. Logo, $c = ma - na = (m - n)a = ka$, para algum $k \in$ e, portanto, $a \mid c$.

v) $a \mid b$ e $b \mid c$ implicam $b = ma$ e $c = nb$, onde $m, n \in$. Assim:

$$c = nb \text{ implica } c = n(ma) = (nm)a, \text{ portanto, } a \mid c.$$

Proposição 2. Sejam $a, b, c, d \in$, com $a, c \neq 0$. Se $a \mid b$ e $c \mid d$, então $ac \mid bd$.

Demonstração: $a \mid b$ e $c \mid d$ implicam $b = ma$ e $d = nc$, com $m, n \in$. Assim, $bd = (ma)(nc) = (mn)ac = k(ac)$, para algum $k \in$. Portanto, $ac \mid bd$.

Observação: Em particular, se $b \mid a$, então $bc \mid ac$, para todo $c \in - \{0\}$.

Proposição 3. Se a é múltiplo de b e vale a recíproca, então $a = b$, para todo $a, b \in$.

Demonstração: $a = mb$ e $b = na$, para $m, n \in$. Portanto, $m = -$ e $n = -$. Daí, $mn = -$. $- = 1$ se, e somente se, $m = n = 1$. Portanto, $- = 1$ se, e somente se, $a = b$.

Exemplo 1. Mostre que, se para algum $n \in$, $m \mid (35n + 26)$, $m \mid (7n + 3)$ e $m > 1$, então $m = 11$.

Resolução: Usando o item **iii)** da **Proposição 1**, temos que, para algum $n \in$:
$m \mid (35n + 26)$ e $m \mid (7n + 3)$ implicam $m \mid (35n + 26) - (7n + 3) = 28n + 23$. Mas:
$28n + 23 = 22n + 22 + (6n + 1) = 11(2n + 2) + (6n + 1) = 11k + (6n + 1)$, onde $k = (2n + 2)$.

Então, $m \mid 28n + 23$ se, e somente se, $m \mid 6n + 1$, para algum $n \in$. Por exemplo, para $n = 9$, temos: $6n + 1 = 6 \times 9 + 1 = 55 = 5 \times 11$. Assim, $m \mid 6n + 1$ implica $m \mid 11$. Logo, $m = 1$ ou $m = 11$. Como $m > 1$, segue que $m = 11$.

Outra maneira: Temos: $m \mid (35n + 26)$ e $m \mid (7n + 3)$, para algum $n \in$. Logo, existem $a, b \in$, tais que:

$$35n + 26 = ma \text{ e } 7n + 3 = bm$$

$$35n + 26 = ma \text{ e } 7 \times 5n + 3 \times 5 = 5bm$$

$$(a - 5b)m = 11$$

$$m = 11/(a - 5b).$$

Daí, $a - 5b = 1$ ou $a - 5b = 11$. Em qualquer um dos casos, estas equações têm solução em . Basta tomar $b = 1$, por exemplo. Como $m > 1$, por hipótese, conclui-se que $m = 11$.

Exemplo 2. Para que valores de $n \in$:

a) $(n - 2)$ divide $2n$?

Resolução: Como $(n-2) \mid 2n$, então, existe $k \in$, tal que $2n = (n-2)k$. Isto equivale a $n = 2k/(k-2)$.

Para que $n \in$, devemos ter $k = 3$, 4 ou 6. Daí, segue que $n = 6$, 4 ou 3. Note que à medida em que o valor k aumenta (em **)**, o valor de n diminui em .

Outra maneira: note que $2n = (n-2)2 + 4$. Daí, $(n-2) \mid 2n$ se, e somente se, $(n-2) \mid 4$. Isto equivale a $n - 2 = 1$, 2 ou 4, ou seja, $n = 3$, 4 ou 6.

b) $(n-2)$ divide $(n+2)$?

Resolução: $(n-2) \mid (n+2)$, então, existe $k \in$, tal que $(n+2) = (n-2)k$. Isto equivale a $n = 2(k+1)/(k-1)$.

Portanto, $k = 2$, 3 ou 5. Daí, segue que $n = 6$, 4 ou 3. Além disso, à medida que o valor k aumenta (em **)**, o valor de n diminui em .

Outra maneira. Note que $n + 2 = (n-2)1 + 4$. Daí, $(n-2) \mid (n+2)$ se, e somente se, $(n-2) \mid 4$. Isto equivale a $n - 2 = 1$, 2 ou 4, ou seja, $n = 3$, 4 ou 6.

c) $(n-2)$ divide $n^2 + 3$?

Resolução: Dividindo-se $n^2 + 3$ por $n - 2$, obtém-se:

$$n^2 + 2 = (n+2)(n-2) + 1 = (n-2)k + 1, \text{ onde } k = (n+2).$$

Assim, $(n-2) \mid n^2 + 3$ se, e somente se, $(n-2) \mid 1$. Isto equivale a $n - 2 = 1$ e, portanto, $n = 3$.

d) $n + 1$ divide $n^2 + 1$?

Resolução: Dividindo-se $n^2 + 1$ por $n + 1$, obtém-se:

$$n^2 + 1 = (n+1)(n-1) + 2 = (n+1)k + 2, \text{ onde } k = n - 1.$$

Assim, $(n + 1) \mid n^2 + 1$ se, e somente se, $(n + 1) \mid 2$. Isto equivale a $n + 1 = 1$ ou 2 e, portanto, $n = 0$ ou 1.

e) $n - 2$ divide $n^3 + 4$?

Resolução: Dividindo-se $n^3 + 4$ por $n - 2$, obtém-se:

$$n^3 + 4 = (n^2 + 2n + 4)(n-2) + 12 = (n-2)k + 12, \text{ onde } k = n^2 + 2n + 4.$$

Assim, $n - 2 \mid n^3 + 4$ se, e somente se, $n - 2 \mid 12$. Isto equivale a $n - 2 = 1, 2, 3, 4, 6$ ou 12. Portanto, $n = 3, 4, 5, 6$ ou 8.

Exemplo 3. Mostre que 7 divide $10k + j = 5 \times 2k + j$ se, e somente se, 7 divide $k - 2j$.

Resolução: ( ) $7 \mid 10k + j$ implica $10k + j = 7q$ e, portanto, $j = 7q - 10k$. Daí:

$$k - 2j = k - 2(7q - 10k) = 21k - 14q = 7(3k - 2q) = 7n.$$

Assim, $7 \mid k - 2j$.

( ) $7 \mid k - 2j$ implica $k - 2j = 7q$ e, portanto, $k = 7q + 2j$. Daí:

$$10k + j = 10(7q + 2j) + j = 70q + 21j = 7(10q + 3j) = 7n.$$

Portanto, $7 \mid 10k + 2j$.

Uma propriedade relevante dos números naturais é que não existe número natural entre dois números naturais consecutivos. A partir disso, decorre outra importante propriedade, a saber:

Propriedade Arquimediana. Dados $a, b \in$, com $b \neq 0$, existe $n \in$, tal que $bn > a$.

Demonstração: Temos: $b \in$ = {1, 2, 3, ...} implica $b \geq 1$. Mas, $a \in$ implica $a + 1 \in$. Daí, fazendo $n = a + 1$, segue que:

$$bn = b(a + 1) = ba + b \geq a + 1 > a.$$

Proposição 4 (Limitação). Sejam $a, b \in$, com $b \neq 0$. Se $b \mid a$, então $b \leq a$.

Demonstração: $b \mid a$ implica $a = ma$, onde $m \in$. Mas, $m \in$ implica $m \geq 1$ e, portanto, $mb \geq b$. Assim, $a \geq b$.

Outra maneira de justificar esse fato: como $b \in$ – {0}, então $b \geq 1$. Assim, existe $n \in$, tal que $b = 1 + n$.

Por outro, $b \mid a$. Então, existe $m \in$ – {0}, tal que $a = mb$. Dessa forma:

$$a = m(1 + b) = m + mb \text{ e, portanto, } a \geq b.$$

Observação: A recíproca da propriedade da limitação não é verdadeira, pois, não é verdade que $b \leq a$ implica $b \mid a$. De fato, por exemplo: $5 \geq 3$, mas 3 não divide 5.

Não obstante, a divisibilidade é uma *relação de ordem*, pois, valem as propriedades *reflexiva*, *transitiva* e *antissimétrica*.

***Reflexiva*:** qualquer que seja $a \in$, $a \mid a$.

***Transitiva*:** para todo $a, b \in$, $a \mid b$ e $b \mid c$ implicam $a \mid c$. (Retomar a demonstração **v) da Proposição 1**)

***Antissimétrica*:** para todo $a, b \in$, $a \mid b$ e $b \mid a$ implicam $a = b$. (Usar a proposição da limitação)

Exemplo 4. Determinar o menor número natural n, tal que $4n^2 + 1$ seja divisível por 65.

Resolução: Pela propriedade da limitação, temos: $65 \mid 4n^2 + 1$ implica $65 \leq 4n^2 + 1$ e, portanto, $n^2 \geq 16$. Daí, $n \geq 4$. Como n é o menor possível, segue que $n = 4$.

Exemplo 5. Mostre que existem infinitos múltiplos de 65 da forma $4n^2 + 1$.

Resolução: Para $n = 4$, temos: $4n^2 + 1 = 4 \times 4^2 + 1 = 65$. Seja $n = 4 + a$, onde $a \in$. Assim:

$$\begin{aligned} 4n^2 + 1 &= 4(4 + a)^2 + 1 \\ &= 4a^2 + 32a + 65 \\ &= a(4a + 32) + 65. \end{aligned}$$

Dessa forma, $4n^2 + 1$ é múltiplo de 65 se, e somente se, 65 divide a, ou seja, $a = m.65$, para algum $m \in$. Assim, $n = 4 + a$ implica $n = m.65 + 4$, para todo $m \in$.

Portanto, $n = m.65 + 4$, com $m \in$ gera infinitos múltiplos de 65.

Exemplo 6. Mostre que se um dado número divide um número da forma $4n^2 + 1$, então, ele dividirá uma infinidade desses números. Para o resultado obtido, existe algo de especial dos números da forma $4n^2 + 1$? Verifique o resultado para os números da forma $an^2 + bn + c$, onde $a, b, c \in$, com a e b não simultaneamente nulos.

Resolução: Seja $m \in$ = {1, 2, 3, ...}, tal que $m \mid 4n^2 + 1$. Fazendo $f = m + r$, onde $r \in$, temos:

$$\begin{aligned} 4n^2 + 1 &= 4f^2 + 1 \\ &= 4(m + r)^2 + 1 \\ &= 4m^2 + 8mr + 4r^2 + 1 \\ &= m(4m + 8r) + 4r^2 + 1. \end{aligned}$$

Assim, $m \mid 4n^2 + 1$ se, e somente se, $m \mid 4r^2 + 1$.

Existe algo de especial sim, pois, para m e $m + r$, onde $m, r \in$, temos:

$$m \mid 4n^2 + 1 \qquad m \mid 4r^2 + 1.$$

Agora, para a expressão $an^2 + bn + c$, suponhamos que $m \mid af^2 + bf + c$. Então, fazendo $f = m + r$, com $r \in$, temos:

$$\begin{aligned} af^2 + bf + c &= a(m + r)^2 + b(m + r) + c \\ &= m(am + 2ar + b) + ar^2 + br + c. \end{aligned}$$

Portanto:

$$m \mid af^2 + bf + c \qquad m \mid ar^2 + br + c.$$

Um método de demonstração utilizado em proposições referente a números naturais é o Princípio (ou Axioma) de Indução Matemática, descrito a seguir:

Princípio (ou Axioma) de Indução Matemática

Dada uma *sentença aberta* $P(n)$, com $n \in$ $_0$ = {0, 1, 2, ...} e suponha que $a \in$ $_0$, de modo que:

i) $P(a)$ é verdade (*verificar*); e

ii) Para todo $n \in$ $_0$, $P(n)$ implica $P(n + 1)$ é verdade (*demonstrar*). Então, segue que $P(n)$ é verdadeira, para todo $n \geq a$.

Demonstração: Seja um subconjunto $S = \{n \in$ $_0$; $P(n)\}$ de $_0$, tal que $P(n)$ é uma *sentença aberta* verdadeira. Considere o conjunto $E_m = \{m \in$ $_0$; $(a + m) \in S\}$. Então:

$$a + E_a = \{a \in \text{ }_0 \text{ ; } a + a = 2a = n \in S\}.$$

Logo, $a + E_a$ é subconjunto de S. Assim, para todo $k \in (a + E_a)$ implica $k \in S$. Em particular, **i)** para $m = 0$, temos:

$$a + m = a + 0 = a = n \in S \text{ e, portanto, } 0 \in E_m.$$

Por outro lado, **ii)** se $m \in E_m$, então $a + m \in S$. Daí, $(a + m) + 1 \in S$. Logo, $m + 1 \in E_m$.

Assim, pelo Princípio de Indução Matemática, seque que $E_m = \ _0$. Portanto, para todo $m \geq a$, o conjunto $\{a \in \ _0 ; m \geq a\} = a + \ _0 \subset S$.

Para dar um sentido preciso a sentenças abertas referentes a números naturais, utilizando o Princípio de Indução Matemática, escreve-se, por recorrência, uma expressão E_n, com $n \in a + \ _0$, da forma:

Primeiro: define-se E_a , para $a \in \ _0$.

Segundo: demonstra-se, a partir E_n, como obter E_{n+1}, para todo $n \in a + \ _0$.

Exemplo 7. (Definição de Progressão Aritmética) Uma *progressão aritmética* é uma sequência de números reais $(a_n) = (a_1, a_2, a_3, \ldots , a_n, \ldots)$, com $n \in$, tal que:

i) a_1 é dado; e

ii) $a_{n+1} = a_n + r$, onde r um número real fixo chamado *razão*.

Mostre que $\boldsymbol{a_n = a_1 + (n - 1)r}$.

Resolução:

i) Para $n = 1$, temos: $a_1 = a_1 + (1 - 1)r = a_1$.

ii) Suponha que $a_n = a_1 + (n - 1)r$, para algum $n \in$. Vamos demonstrar que vale também para $n + 1$. Temos:

$$a_{n+1} = a_n + r = a_1 + (n - 1)r + r = a_1 + [(n - 1) + 1]r.$$

Assim, pelo Princípio de Indução Matemática, $a_n = a_1 + (n - 1)r$ vale para todo $n \in$.

Exemplo 8. a) Mostre que $1 + 2 + 3 + \ldots + n = n(n + 1)/2$, para todo $n \in$.

Resolução: Para $n = 1$, temos: $1 = 1(1 + 1)/2$.

Suponha que, para algum $n = k$, $1 + 2 + 3 + \ldots + k = k(k + 1)/2$. Assim, para $n = k + 1$, temos:

$$\begin{aligned} 1 + 2 + 3 + \ldots + k + (k + 1) &= k(k + 1)/2 + (k + 1) \\ &= (k + 1)(1 + k/2) \\ &= (k + 1)[(k + 1) + 1]/2. \end{aligned}$$

Logo, pelo Princípio de Indução Matemática $1 + 2 + 3 + \ldots + n = n(n + 1)/2$, para todo $n \in$.

b) Mostre que $n(n + 1)/2$ é um número natural, para todo $n \in$.

Resolução: Pelo princípio da paridade, $n = 2k$ número par) ou $n = 2k + 1$ (número ímpar), onde $k \in$.

Se $n = 2k$, temos: $n(n + 1)/2 = 2k(2k + 1)/2$

$$= k(2k + 1) \in .$$

Se $n = 2k + 1$, segue que: $n(n + 1)/2 = (2k + 1)(2k + 1 + 1)/2$

$$= (2k + 1)2(k + 1)/2$$

$$= (2k + 1)(k + 1) \in .$$

Portanto, em qualquer um dos casos, temos $n(n + 1)/2 \in$.

Exemplo 9. Quantos números naturais entre 1 e 1000 são divisíveis por 9?

Resolução: Os números entre 1 e 1000 divisíveis por 9 são: 9, 18, 27, ... , 999. Note que esta sequência é uma progressão aritmética de razão e primeiro termo, ambos, iguais a 9. Assim:

$$a_n = a_1 + (n-1)r \qquad 999 = 9 + (n-1)9 \qquad n = 111.$$

Portanto, há 111 números divisíveis por 9 entre 1 e 1000.

Exemplo 10. (Definição de Progressão Geométrica) Uma *progressão geométrica* é uma sequência de números reais $(a_n) = (a_1, a_2, a_3, \ldots, a_n, \ldots)$, com $n \in$, tal que:

i) a_1 é dado; e

ii) $a_{n+1} = a_n q$, onde q um número real fixo chamado *razão*.

Dessa forma, mostre que $\boldsymbol{a_n = a_1\, q^{n-1}}$. Com efeito:

i) Para $n = 1$, temos: $a_1 = a_1 q^{1-1} = a_1 q^0 = a_1$.

ii) Suponha que $a_n = a_1\, q^{n-1}$, para algum $n \in$. Então:

$$a_{n+1} = a_n q = = a_1\, q^{n-1} q = a_1 q^{(n-1)+1} = a_1 q^{(n+1)-1}.$$

Portanto, pelo Princípio de Indução Matemática, $a_n = a_1 q^{n-1}$, para todo $n \in$.

Exemplo 11. (ENC, MEC/INEP/1998 - adaptado) Quantos são os múltiplos positivos de 6 que se escrevem (no sistema decimal) com dois algarismos?

Resolução: Temos: 6 | , onde $a, b \in \{0, 1, 2, \ldots, 9\}$, implica = m.6, para algum $m \in$. Portanto, $\in \{12, 18, \ldots, 96\}$.

Note que os elementos desse conjunto formam uma progressão aritmética, com primeiro termo 12 e razão 6. Assim, o número de múltiplos positivos de 6 com dois algarismos é: $a_n = a_1 + (n-1)r$ $96 = 12 + (n-1)6$ $n = 15$.

Exemplo 12. Mostre, por indução, que 3 divide $4^n - 1$.

Resolução: Para $n = 1$, temos: $4^n - 1 = 4^1 - 1 = 3$. Suponhamos que $3 \mid 4^k - 1$, para algum $k \in$. Então, para $n = k + 1$, temos:

$$4^{k+1} - 1 = 4.4^k - 1 = 4.4^k - 4 + 4 - 1 = 4(4^k - 1) + 3.$$

Mas, por hipótese de indução, $3 \mid 4^k - 1$. Além disso, $3 \mid 3$, logo, $3 \mid 4^{k+1} - 1$.

Portanto, pelo Princípio de Indução Matemática, 3 divide $4^n - 1$, para todo $n \in$.

Exemplo 13. Mostre, por indução, que 9 divide $10^n - 1$.

Resolução: Para $n = 1$, temos: $10^n - 1 = 10^1 - 1 = 9$. Suponhamos que $9 \mid 10^k - 1$, para algum $k \in$. Então, para $n = k + 1$, temos:

$$10^{k+1} - 1 = 10.10^k - 1 = 10.10^k - 10 + 10 - 1 = 10(10^k - 1) + 9.$$

Mas, por hipótese de indução, $9 \mid 10^k - 1$. Além disso, $9 \mid 9$, logo, $9 \mid 10^{k+1} - 1$.

Portanto, pelo Princípio de Indução Matemática, 9 divide $10^n - 1$, para todo $n \in$.

2.2 Divisão Euclidiana

Dados dois números naturais a e $b \neq 0$, considere a "Tabuada de b" referente à operação de *multiplicação*.

$$0 \times b = 0$$
$$1 \times b = b$$
$$2 \times b = 2b$$
$$3 \times b = 3b$$

$$p \times b = pb$$

Note que o produto $p \times b$ vai se aproximando do número a à medida que p aumenta. Assim, para um certo $q \in$, teremos:

$$q \times b = a \quad \textbf{ou} \quad q \times b < a \text{ e } (q + 1) \times b > a.$$

Isso significa que ou a é múltiplo b ou a está entre dois múltiplos consecutivos de b. Em símbolos, escrevemos:

$$qb \leq a < (q + 1)b.$$

Nessa desigualdade, o número $(q + 1)$ é o menor (ou mínimo) elemento do conjunto $\{k \in$; $bk > a\}$, ou seja, dentre todos os múltiplos maiores do que a, da forma bk, o número $(q + 1)$ é o menor. De fato: considere o conjunto dos múltiplos de b maiores do que a: $\{k \in$; $bk > a\}$. Este conjunto é não vazio, pois:

$$b \in \text{ implica } b \geq 1.$$

Multiplicando por a, ambos os membros dessa desigualdade, obtemos:

$$ab \geq a.$$

Somando b nessa última desigualdade, temos:

$$ab + b \geq a + b \text{ e, portanto, } b(a + 1) \geq a + b > a.$$

Portanto, o número $a + 1$ é o menor elemento do conjunto $\{k \in$; $bk > a\}$.

A desigualdade $qb \leq a$ implica existir $r \in$, tal que $a = bq + r$, com a condição $r < b$. Com efeito: suponhamos o contrário, ou seja, $r \geq b$. Então: $r = a - bq \geq b$ implica $a - bq + bq \geq b + bq$ e, portanto, $a \geq (q + 1)b$, o que é um absurdo! Logo, $r < b$. Isto mostra a *existência* de dois números q e r.

Os números q e r são *únicos*. De fato: suponhamos que exista outro par q^* e r^*. Daí: $a = bq + r = bq^* + r^*$, com $r < b$ e $r^* < b$ implica $bq - bq^* = r - r^*$ e, portanto, $b(q - q^*) = r - r^*$. Assim, $b \mid r - r^*$ se, e somente se, $r - r^* = 0$, ou seja, $r = r^*$.

Como $b > 0$, então, $b(q - q^*) = r - r^* = 0$ se, e somente se, $q - q^* = 0$ e, portanto, $q = q^*$.

Teorema 1. Dados dois números naturais a e $b \neq 0$, existe um único par de números q e r, de modo que $a = bq + r$, com a condição $0 \leq r < b$.

A condição $0 \leq r < b$ indica que os possíveis restos na divisão de a por $b \neq 0$ são: 0, 1, 2, ... , $b - 1$. Além disso, o *maior resto possível* (ou resto máximo) é o número $b - 1$. Em símbolos, escrevemos: $r_{max} = b - 1$.

Exemplo 14. Na divisão de a por $b \neq 0$, mostre que b divide $a - 1$ quando o resto é máximo.

Resolução: Dividindo-se a por b, com resto máximo, obtém-se:

$$a = bq + r_{max}, \text{ com } r_{max} = b - 1.$$

Daí, segue que $a = bq + r_{max} = bq + b - 1 = (q + 1)b - 1 = kb - 1$ e, portanto, $a + 1 = kb$, onde $k = q + 1$ implica $b \mid a + 1$.

Exemplo 15. Na divisão de 27 por 5, determinar o quociente e o resto.

Resolução: Como $b = 5$, então, os possíveis restos são 0, 1, 2, 3 e 4. Mas: $r = a - bq \geq 0$, onde $a = 27$ e $b = 5$. Portanto, $27 - 5q \geq 0$ implica $q \leq 5$, ou seja, $q = 5$ (maior). Assim, $r = 27 - 5q = 27 - 5\times5$ e, portanto, $r = 2$.

Como $b = 5$, então, os possíveis restos são 0, 1, 2, 3 e 4. Mas: $r = a - bq \geq 0$, onde $a = 27$ e $b = 5$. Portanto, $27 - 5q \geq 0$ implica $q \leq 5$, ou seja, $q = 5$ (maior). Assim, $r = 27 - 5q = 27 - 5\times5$ e, portanto, $r = 2$.

Exemplo 16. Mostre que, para todo $n \in$:

a) se n é ímpar, então $n^2 - 1$ é divisível por 8.

b) 4 *não* divide $n^2 + 2$.

Resolução: a) Por hipótese, n é ímpar. Então, $n = 2k + 1$, onde $k \in$. Assim:

$$n^2 - 1 = (2k + 1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k^2 + 4k = 4k(k + 1).$$

Observe que, em um produto de dois números naturais consecutivos $k(k + 1)$, um dos fatores sempre é um número par, ou seja, $k(k + 1) = 2q$, onde $q \in$. Dessa forma:

$$n^2 - 1 = 4k(k + 1) = 4\times2q = 8q \text{ implica } 8 \mid n^2 - 1.$$

b) Como $n \in$, então, pelo princípio da paridade (é a característica de um número ser par ou ímpar), ou $n = 2k$ (número par) ou $n = 2k + 1$ (número ímpar), onde $k \in$. Assim:

i) para $n = 2k$, temos:

$$n^2 + 2 = (2k)^2 + 2 = 4k^2 + 2 \text{ implica } 4 \nmid 2 \text{ e, portanto, 4 } \textit{não} \text{ divide } n^2 + 2.$$

ii) para $n = 2k + 1$, segue que:

$$n^2 + 2 = (2k + 1)^2 + 2 = 4k^2 + 4k + 1 + 2 = 4(k^2 + k) + 3 = 4q + 3, \text{ onde } q \in .$$

Como $4 \nmid 3$, então, 4 *não* divide $n^2 + 2$.

Em relação ao **Exemplo 13**, há uma outra maneira de resolver. Vejamos:

$$10^n = (9 + 1)^n = m.9 + 1.$$

Daí, segue que $10^n - 1 = m.9$, para algum $m \in$. Portanto, 9 divide $10^n - 1$, para todo $n \in$.

Note que, $10^n = m.9 + 1$, para algum $m \in$. Isto significa que o *resto* da divisão de 10^n por 9 é sempre 1, qualquer que seja $n \in$.

Outro fato curioso é:

$$111 \ldots 1 \text{ (com } n \text{ uns)} = 10^{n-1} + \ldots + 10 + 1.$$

Observe que a soma à direita da igualdade acima é uma progressão geométrica, com primeiro termo igual a 1 e razão igual a 10. Assim:

$$\begin{aligned} 111 \ldots 1 \text{ (com } n \text{ uns)} = 10^{n-1} + \ldots + 10 + 1 &= a_1[(q^n - 1)/(q - 1)] \\ &= 1(10^n - 1)/(10 - 1)] \\ &= (10^n - 1)/9. \end{aligned}$$

Dessa forma, $(10^n - 1)/9 = 111 \ldots 1$ (com n uns) é um número natural e, portanto, 9 divide $10^n - 1$. Além disso, temos:

$$(10^n - 1)/9 = 111 \ldots 1 \text{ (com } n \text{ uns)} \qquad 10^n - 1 = 999 \ldots 9 \text{ (com } n \text{ noves).}$$

Exemplo 17. Mostre que, dados m múltiplos consecutivos, um e apenas um deles é múltiplo de m.

Resolução: Pelo **Teorema 1**, *todo número* $n \in$ *pode ser escrito da forma* $n = mk + r$, com $0 \leq r \leq m - 1 = r_{max}$ e k, r únicos. Assim, os múltiplos consecutivos de m são:

$$mk,\ mk + 1,\ mk + 1, \ldots, mk + r_{max}.$$

Para $r = 0$ e pela *unicidade* do resto, temos: $n = mk + r$ implica $n = mk$, que é um múltiplo de m.

Exemplo 18. a) Quantos são os múltiplos de 5 entre 1 e 246? **b)** Dados $0 < a \leq n \in$, mostre que no intervalo [1, n] existem q múltiplos de a, onde q é o quociente da divisão de n por a.

Resolução: a) Pelo **Teorema 1**, temos: $246 = 5\times49 + 1$ e, portanto, $245 = 5\times49$. Assim, os múltiplos de 5 **entre** 1 e 246 são:

$$5\times\mathbf{1},\ 5\times\mathbf{2},\ 5\times\mathbf{3}, \ldots, 5\times\mathbf{49} \text{ implica } \mathbf{1}, \mathbf{2}, \mathbf{3}, \ldots, \mathbf{49}.$$

A sequência **1**, **2**, **3**, ... , **49** tem 49 números e, portanto, 49 múltiplos de 5 **entre** 1 e 246.

b) Os múltiplos de a no intervalo [1, n] são:

$$1\times a,\ 2\times a,\ 3\times a, \ldots, (k-1)a,\ ka, \text{ onde } ka \leq n.$$

Nessa sequência, há k múltiplos de a. Assim, temos que mostrar que $q = k$. De fato: na divisão de n por a, existe um único par de números q e r, tal que:

$$n = aq + r, \text{ com } 0 \leq r < a.$$

Mas, $ka \leq n = aq + r$ implica $ka - aq = r$. Como $0 \leq r < a$, então, $ka - aq = 0$ e, portanto, $ka = aq$, com $a > 0$, por hipótese. Assim, $q = k$.

Nota: em geral, a parte inteira da divisão de n por a indica-se por $q = [n/a]$.

c) Dados $0 < a \leq n < m \in$, mostre que no intervalo [n, m] existem $q_1 - q$ múltiplos de a, onde q_1 é o quociente da divisão de m por a e q é o quociente da divisão de n por a.

Resolução: Na divisão de m por a, temos:

$$m = aq_1 + r, \text{ com } 0 \leq r_1 < a.$$

Assim, há duas possibilidades:

i) n é múltiplo de a: supondo que $n = aq$. Então, todos os múltiplos de a no intervalo [n, m] são:

$$aq,\ a(q+1),\ a(q+2),\ a(q+3),\ \ldots,\ a(q_1-1),\ aq_1\ (r_1=0).$$

Portanto, há $(q_1 - q) + 1$ múltiplos de a no intervalo $[n, m]$.

ii) n não é múltiplo de a: supondo que $n = aq + r$, com $0 < r < a$. Então, todos os múltiplos de a no intervalo $[n, m]$ são:

$$a\mathbf{(q+1)},\ a\mathbf{(q+2)},\ a\mathbf{(q+3)},\ \ldots,\ a\mathbf{(q_1-1)},\ a\mathbf{q_1}\ (r_1=0).$$

Assim, há $[q_1 - (q + 1)] + 1 = q_1 - q$ múltiplos de a no intervalo $[n, m]$.

Exemplo 19. (ENC/2001) Seja um número natural n. Mostre que a divisão de n^2 por 6 nunca deixa resto 2.

Resolução: Pelo **Teorema 1**, *todo número* $n \in$ *pode ser escrito da forma* $n = 6q + r$, onde $0 \leq r < 6$, isto é: $r = 0, 1, 2, 3, 4$ ou 5. Mas:

$$n^2 = (6q + r)^2 = m6 + r^2.$$

Daí, para $r = 0, 1, 2, 3, 4$ ou 5, temos, respectivamente, os únicos restos: $0 ; 1 ; 4 ; 3 ; 4 ; 1$. Portanto, nunca deixa resto 2.

Exemplo 20. Qual é o menor múltiplo de 5 que deixa resto 2, quando dividido por 3 e 4?

Resolução: Pelo **Teorema 1**, podemos escrever: $n = m.3 + 2$ e $n = m.4 + 2$, com n sendo o menor múltiplo de 5. Isto equivale a $n - 2 = m.3$ e $n - 2 = m.4$. Assim, para condicionar ao menor múltiplo, tomamos:

$$n - 2 = k \times mmc(3, 4) \qquad n = 12k + 2 \qquad n = (10 + 2)k + 2 \qquad n = 10k + 2(k + 1).$$

Assim, $n = 10k + 2(k + 1) = m.5 + 2(k + 1)$. Então, n é múltiplo de 5 se, e somente se, $2(k + 1) = m.5$. Mas, n deve ser o menor múltiplo de 5. Para que isso aconteça, $m = 2$. Daí, $2(k + 1) = 10$ e, portanto, $k = 4$. Logo, $n = 12k + 2 = 12\times4 + 2$ e, portanto, $n = 50$.

Uma aplicação importante do algoritmo da divisão está relacionada à escrita de um número numa base $b > 1$.

2.3 Sistema de Numeração Posicional

No sistema de numeração decimal posicional (base 10), todo número $N = r_n r_{n-1} \ldots r_1 r_0$ pode ser escrito de forma única como:

$$N = 10^n r_n + 10^{n-1} r_{n-1} + \ldots + 10 r_1 + 10^0 r_0,$$

onde os r_j são algarismos, tais que $r_j \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Isso pode ser generalizado pelo teorema a seguir, utilizando o **Teorema 1**.

Teorema 2. Seja um número natural $b > 1$. Então, todo número $N = (r_n r_{n-1} \ldots r_1 r_0)_b$ pode ser escrito na base b, de modo único, na forma:

$$N = b^n r_n + b^{n-1} r_{n-1} + \ldots + b^1 r_1 + b^0 r_0.$$

onde os r_j são algarismos, tais que $r_j \in \{0, 1, 2, \ldots, b - 1\}$.

Demonstração: (*Existência)* Suponha que b não divide N. Então, pelo **Teorema 1**, temos:

$$N = bq_0 + r_0, \quad r_0 < b$$

$$q_0 = bq_1 + r_1, \quad r_1 < b$$

$$q_1 = bq_2 + r_2, \quad r_2 < b$$
$$q_2 = bq_3 + r_3, \quad r_3 < b$$

Como $N > q_0 > q_1 > q_2 > \ldots$, então, em algum momento dessa expansão, devemos ter $q_{n-1} < b$ e, portanto:

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

Isso acarreta que $q_n = 0$ e, por conseguinte, $q_n = q_{n+1} = q_{n+2} = q_{n+3} = ... = 0$. Logo, $r_{n+1} = r_{n+2} = r_{n+3} = ... = 0$. Assim:

$$N = b^n r_n + b^{n-1} r_{n-1} + ... + b^1 r_1 + b^0 r_0.$$

(*Unicidade)* Suponha que:

$$N = b^n r_n + b^{n-1} r_{n-1} + ... + b^1 r_1 + b^0 r_0 = b^n r'_n + b^{n-1} r'_{n-1} + ... + b^1 r'_1 + b^0 r'_0.$$

Então:

$$(b^n r_n - b^n r'_n) + (b^{n-1} r_{n-1} - b^{n-1} r'_{n-1}) + ... + (b^1 r_1 - b^1 r'_1) + (b^0 r_0 - b^0 r'_0) = 0$$
$$b^n(r_n - r'_n) + b^{n-1}(r_{n-1} - r'_{n-1}) + ... + b^1(r_1 - r'_1) + (r_0 - r'_0) = 0.$$

Como b > 1, segue que:

$$r_n - r'_n = 0,\ r_{n-1} - r'_{n-1} = 0,\ r_1 - r'_1 = 0,\ r_0 - r'_0 = 0 \qquad r_n = r'_n,\ r_{n-1} = r'_{n-1},\ ...,\ r_0 = r'_0.$$

Esse teorema mostra como expressar um número natural qualquer na base b.

No caso do *Sistema de Numeração Posicional Decimal*, a base é 10 ($b = 10$) e $r_j \in \{0, 1, 2, ... , 9\}$.

Assim, $N = (r_n r_{n-1} ... r_1 r_0)_b = (r_n r_{n-1} ... r_1 r_0)_{10}$ ou $N = r_n r_{n-1} ... r_1 r_0$. Dessa forma, $N = 10^n r_n + 10^{n-1} r_{n-1} + ... + 10 r_1 + 10^0 r_0 = 10^n r_n + 10^{n-1} r_{n-1} + ... + 10 r_1 + r_0$. Assim:

$$N = r_n r_{n-1} ... r_1 r_0 = 10^n r_n + 10^{n-1} r_{n-1} + ... + 10 r_1 + r_0.$$

Observações:

1) A potência 10^n, para todo $n \geq 1$, é um número par. De fato:

$$10^n = (2 \times 5)^n = 2^n \times 5^n = 2(2^{n-1} \times 5^n) = 2k, \text{ onde } k = 2^{n-1} \times 5^n, \text{ para todo } n \geq 1.$$

2) $10^n = 9k + 1$ ou $3h + 1$, para todos $n \geq 1$. Com efeito:

$$10^n = (9 + 1)^n = 9^n + m.9 + 1^n = 9(9^{n-1} + m) + 1 = 9k + 1 \text{ ou } 3 \times 3k + 1 = 3h + 1.$$

Exemplo 21. Num sistema de numeração de base $b > 1$, quantos números existem formados de n algarismos? E qual é o menor deles?

Resolução: Todo número natural N pode ser escrito, numa base $b > 1$, da seguinte forma:

$$N = b^n r_n + b^{n-1} r_{n-1} + ... + b^1 r_1 + b^0 r_0,$$

onde os r_j são algarismos, tais que $r_j \in \{0, 1, 2, ... , b - 1\}$.

O primeiro número com n algarismos é b^{n-1}, e o último, é $b^n - 1$. Assim, de $b^n - 1$ a b^{n-1} existem $(b^n - 1) - b^{n-1} + 1$ números, ou seja:

$$(b^n - 1) - b^{n-1} + 1 = b^n - b^{n-1}$$
$$= b^n - b^n/b$$
$$= b^n(1 - 1/b)$$
$$= b^n/b(b - 1)$$
$$= (b - 1)b^{n-1}.$$

Como $b > 1$ e n é natural, temos: $b^n - 1 \geq b^{n-1}$. Portanto, o menor deles é b^{n-1}.

3. CONCLUSÃO

A teoria elementar de Aritmética apresentada possui imensa variedade de conceitos, proposições e teoremas.

Com isso, surge a possibilidade de desenvolver técnicas e habilidades em demonstrações de proposições de Matemática. Por esta razão, toma-se a Aritmética é como ponto de partida para construir tais procedimentos, pois, de modo simples, a teoria se apresenta e, gradativamente, torna-se complexa, o que possibilita aprofundamento para a aprendizagem em demonstrações de proposições matemáticas. Em particular, destaca-se o Princípio de Indução Matemática como uma forma de justificar proposições referente a números naturais. Além disso, o Teorema atinente à Divisão Euclidiana, e também à forma de operar a divisão utilizando-se a "Tabuada de Multiplicação", onde destacamos a existência e unicidade do quociente e resto.

Assim, as habilidades de demonstrações em Matemática podem ser adquiridas por meio da Aritmética Elementar.

4. REFERÊNCIAS

ALENCAR FILHO, Edgard de. **Teoria Elementar dos Números**. São Paulo, 1992.

COLEÇÃO PROFMAT. **Tópicos de Teoria dos Números**. Rio de Janeiro – SBM, 2012.

DOMINGUES, H.H. **Fundamentos de Aritmética**. São Paulo, 1991.

ENZO R. Gentile. **Aritmética Elemental**. Buenos Aires, Argentina, 1985.

HEFEZ A. **Elementos de Aritmética**. Rio de Janeiro – SBM, 2004.

OLIVEIRA, Krerley Irraciel Martins e FERNÁNDEZ, Adán José Corcho. **Iniciação à Matemática: um curso com problemas e soluções**. Rio de Janeiro – SBM, 2010.