UNIVERSIDADE FEDERAL DO CARIRI
CENTRO DE CIÊNCIAS E TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
EM REDE NACIONAL

FRANCISCO DE ASSIS FERREIRA

A PROVA DOS NOVES, DIVISIBILIDADE E CONGRUÊNCIA

JUAZEIRO DO NORTE
2017

FRANCISCO DE ASSIS FERREIRA

A PROVA DOS NOVES, DIVISIBILIDADE E CONGRUÊNCIA

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional, da Universidade Federal do Cariri, como requisito parcial para obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Orientador:
Prof. Dr. Plácido Francisco de Assis Andrade.

JUAZEIRO DO NORTE
2017

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO CARIRI
CENTRO DE CIÊNCIAS E TECNOLOGIA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

A Prova dos Noves, Divisibilidade e Congruência

Francisco de Assis Ferreira

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional – PROFMAT do Centro de Ciências e Tecnologia da Universidade Federal do Cariri, como requisito parcial para obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática

Aprovada em 21 de julho de 2017.

Banca Examinadora

Prof. Dr. Plácido Francisco de Assis Andrade – UFCA

Orientador

Profa. Dra. Maria Silvana Alcântara Costa - UFCA

Prof. Dr. Valdir Ferreira de Paula Junior - UFCA

Ao meu pai
João Ferreira da Silva
(in memoriam).

A minha mãe Luzia Ana de Lima.

Aos meus filhos Ana Clara e João Pedro.

AGRADECIMENTOS

A Deus, pela sabedoria e humildade concedidas a meu ser.

A meu pai, João Ferreira da Silva, mesmo não estando mais conosco, por ensinar sempre o caminho da verdade, da justiça, do amor e por valorizar a educação e a minha mãe, Luzia Ana de Lima, pelas palavras carinhosas e confortantes diante das adversidades que tal conquista impõe.

Aos meus filhos Ana Clara e João Pedro por alegrarem minha vida com sorrisos e abraços.

Ao amigo Francisco Dias pela parceria de estudos e contribuições à realização desse trabalho.

Aos professores do curso PROFMAT pelas importantes lições de vida e aprendizagem e pelo empenho na construção do meu conhecimento intelectual.

Ao meu professor orientador Dr. Plácido Francisco de Assis Andrade pelas valiosas considerações a este trabalho.

Por fim, à Coordenação de Aperfeiçoamento Pessoal de Ensino Superior(CAPES) pelo apoio financeiro.

"Um matemático que não é também um pouco poeta nunca será um matemático completo." (K. Weierstrass)

RESUMO

O presente trabalho visa resgatar o estudo de divisão de números inteiros positivos através da aplicação e análise da prova do "noves fora". Este método utilizado pela escola antiga, para verificar se uma certa operação, adição ou multiplicação por exemplo, está correta ou não e que hoje ficou relegado ao esquecimento traz ferramentas poderosas de divisibilidade, sistema de numeração e congruência. Mostraremos o método prático da prova dos noves para as operações de adição, subtração, divisão e multiplicação bem como as demonstrações necessárias. Assim é abordado nessa obra o sistema de numeração decimal e mudança de base, algoritmo da divisão, critérios de divisibilidade e congruência. Por fim, conclui-se que a regra não consiste apenas de uma prática social e sim de um instrumento aritmético capaz de desenvolver aprendizagem significativa em matemática.

Palavras-chave: Noves fora. Divisibilidade. Congruência.

ABSTRACT

The present work aims to recover the study of division of positive integers through the application and analysis of the “ noves out ” test. This method used by the old school to verify if a certain operation, addition or multiplication for example, is correct or not and that today was relegated to oblivion brings powerful tools of divisibility, numbering system and congruence. We will show the practical method of the nines test for addition, subtraction, division and multiplication operations as well as the necessary demonstrations. Thus, the system of decimal numbering and base change, division algorithm, divisibility criteria and congruence are discussed in this work. Finally, we conclude that the rule consists not only of a social practice but of an arithmetic instrument capable of developing meaningful learning in mathematics.

Keywords: Nine-out. Divisibility. Congruence.

SUMÁRIO

1 INTRODUÇÃO

A Aritmética sempre foi uma área importante no ensino de Matemática. É notório o conhecimento, de nossos parentes que vivenciaram a escola antiga, das operações básicas. A prova dos noves fora que remota a séculos, foi uma prática muito utilizada para verificar se uma certa operação fundamental estava ou não correta. O processo era repassado também de forma empírica entre as gerações sendo muito comum a prática pelos comerciantes. Por exemplo, para se verificar se a adição $321 + 25 = 346$ estava correta era feito o seguinte procedimento: Somava-se os dígitos das parcelas $(3+2+1+2+5 = 13)$ e se verificava o resto da divisão por 9 do número formado, no caso 4. Da mesma forma, procedia-se com o resultado $(3 + 4 + 6 = 13)$ que também tem resto 4 na divisão por 9. Sendo os restos da soma das parcelas e do resultado iguais, dizia-se está correta a adição.

Neste trabalho foi realizado um estudo sobre a prova dos noves, a temática partiu de um incomodo sobre observações da possível infabilidade do método para garantir exatidão das operações básicas. Na abordagem foi alavancado os aspectos históricos e a importância matemática nos conceitos de divisibilidade e congruência. A princípio, focou-se numa breve reflexão da relevância da prova dos noves como uma prática social, regra, técnica ou método. Mostra-se também como se dá o emprego da regra nas operações de adição, subtração, multiplicação e divisão. Ressalta-se as controvérsias do emprego da técnica evidenciando que nem sempre a mesma é eficaz. Expõe-se aplicações da prova dos noves, dos setes e dos onzes fora utilizando classe de resíduos nos números inteiros.

Em suma, o trabalho mostra a importância da prova dos noves não apenas como prática social, mas como uma poderosa aplicação de conceitos matemáticos de valiosa importância em Aritmética.

2 DIVISIBILIDADE

Neste capítulo estudaremos os axiomas de Peano, o Princípio da Boa Ordenação, as propriedades da divisão, o algoritmo da divisão de Euclides e os critérios de divisibilidade.

2.1 Axiomas de Peano

A construção de números naturais tem como ponto de partida o Sistema Axiomático de Peano constituído por três termos indefinidos e quatro axiomas. No enunciado é assumido a Teoria de conjuntos e o termo número natural deve ser "entendido" como elemento de um conjunto denotado por $\mathbb{N}$.

SISTEMA AXIOMÁTICO DE PEANO

1. Termos indefinidos: Conjunto; número natural; sucessor.
2. Todo número natural tem um único sucessor.
3. Números naturais diferentes tem sucessores diferentes.
4. Existe um único natural, chamado um e representado pelo símbolo 1, que não é sucesso de nenhum outro.
5. Seja X um conjunto de números naturais (isto é $X \subset \mathbb{N}$). Se $1 \in X$ e se, além disso, o sucessor de todo elemento de X ainda pertence a X, então $X = \mathbb{N}$.

O último dos axiomas de Peano é conhecido como *Axioma da indução*. Ele é a base de um eficaz método de demonstração de proposições, método este denominado Princípio de Indução Matemática. O axioma da indução pode ser reescrito, usando-se a liguagem de propriedades. Nesta forma chamamos de Princípio de Indução Matemática.

Teorema 2.1.1 *Seja $P(n)$ uma propriedade relativa ao número natural n. Se*

(i) $P(1)$ é válida e

(ii) para todo $n \in \mathbb{N}$, a validez de P(n) implica na validez de S(n), onde S(n) é o sucessor de n.

então $P(n)$ é válida para todo $n \in \mathbb{N}$.

Demonstração Seja X o subconjunto de números naturais n para os quais $P(n)$ é válida. Em virtude do axioma (i) temos que $1 \in X$ e que $n \in X$ implica $S(n) \in X$, em virtude do axioma (ii). Portanto, pelo axioma da indução, $X = \mathbb{N}$. ∎

Utilizando o termo *sucessor*, ou seja, $S(n) = n + 1$ é definido as operações de adição e multiplicação de naturais. Também é definido uma ordem total, indicada por $\leq$. Para detalhes destas construções ver ([4], pp. 27-31).

Definição 2.1.1 *Seja $X \subset \mathbb{N}$ um conjunto não vazio. Diz-se que $n_1 \in X$ é o menor elemento de X se $n \geq n_1$ para todo $n \in X$.*

Teorema 2.1.2 *Todo subconjunto não vazio $X \subset \mathbb{N}$ possui um menor elemento.*

Demonstração Suponhamos, por absurdo, que X não possua um menor elemento. Seja X' o conjunto complementar de X em $\mathbb{N}$. Considere os conjunto $I_n = \{n \in \mathbb{N}, I_n \subset X'\}$, e a sentença aberta

$$P(n) : I_n \subset X'.$$

Como $1 \leq n$ para todo n, segue-se que $1 \in X'$, pois caso contrário, 1 seria um menor elemento de X, logo $P(1)$ verdade. Supondo que $P(n)$ seja verdade. Se $n+1 \in X$, como nenhum elemento de I_n pertence a X teríamos que $n+1$ é um menor elemento de X, o que contraria a hipótese tomada. Logo, $n+1 \in X'$, seguindo que

$$I_{n+1} = I_n \cup \{n+1\} \subset X',$$

segue que $P(n+1)$ é válido. Pelo princípio de indução matemática $X' = \mathbb{N}$. Logo, X é vazio, uma contradição.

∎

Para a seção seguinte vale ressaltar a importância dos números inteiros que caracterizam-se por não possuir parte decimal. O conjunto dos números inteiros é constituído por todos números naturais e números negativos (números menores que zero). Além disso, o conjunto dos inteiros nos permite trabalhar com a ideia de quantidades negativas.

2.2 Definição e Propriedades de Divisibilidade

Nesta seção relacionaremos algumas propriedades básicas sobre divisibilidade de inteiros as quais serão a base das demonstrações sobre critérios de divisibilidade.

Definição 2.2.2 *Sejam a e b dois números inteiros, com $a \neq 0$. Dizemos que a divide b se, e somente se, existe um inteiro k tal que $b = ak$.*

Para simplificar a escrita, a notação $a \mid b$ indicará que $a \neq 0$ e que a divide b. Observamos que zero é dividido por qualquer inteiro não nulo e não definimos a divisão de um número natural por 0.

Proposição 2.2.1 *Sejam a e b números inteiros. Se $a \mid b$, então*

$$-a \mid b, \qquad a \mid -b, \qquad -a \mid -b \qquad e \qquad |a| \mid |b|.$$

Demonstração Se $a \mid b$, então existe um inteiro k tal que $b = ka$. Além disso, pela Definição 3.1.4 temos $a \neq 0$. Assim, segue que

(i) Do fato de $a \neq 0$, conclui-se que $-a \neq 0$. Logo, $b = (-k)(-a)$. Portanto, $-a \mid b$.

(ii) Como $b = ka$, temos $-b = (-k)a$. Daí, $a \mid -b$.

(iii) Como $-a \neq 0$, então $-b = k(-a)$. Logo, $-a \mid -b$.

(iv) Sendo $a \neq 0$ e $-a \neq 0$, temos $|a| \neq 0$. Assim, $|b| = |k||a|$. Portanto, $|a| \mid |b|$.

■

Proposição 2.2.2 *Sejam a, b e c números inteiros.*

(i) Se $a \mid b$ e $b \mid c$, então $a \mid c$

(ii) Se $a \mid b$ e $b \mid a$, então $a = b$ ou $a = -b$;

(iii) Se $a \mid b$ e $a \mid c$, então $a \mid pb + qc$;

(iv) Se $a \mid b$ e $a \mid b + c$, então $a \mid c$.

Demonstração (i) Se $a \mid b$ e $b \mid c$, então existem p e q inteiros tais que $b = pa$ e $c = qb$, daí segue que $c = (pq)a$. Portanto, $a \mid c$.

(ii) Se $a \mid b$ e $b \mid a$, então existem inteiros r_1 e r_2 tais que $b = r_1 a$ e $a = r_2 b$. Daí, seque $a = r_2 \cdot r_1 a$ implicando em $r_1 \cdot r_2 = 1$. Assim, temos

$$r_1 = r_2 = 1 \qquad ou \qquad r_1 = r_2 = -1.$$

Portanto, $a = b$ ou $a = -b$.

(iii) Se $a \mid b$ e $a \mid c$, então existem inteiros u e v tais que $b = au$ e $c = av$, multiplicando as equações, respectivamente, por p e q temos

$$pb = pua \qquad \text{e} \qquad qc = qva,$$

somando-se as equações membro a membro obtemos $pb + qc = (pu + qv)a$. Portanto, $a \mid (pb + qc)$.

(iv) Se $a \mid b$ e $a \mid b + c$, então existem p e q inteiros tais que $b = ap$ e $b + c = aq$ daí segue que $c = (q - p)a$, portanto, $a \mid c$. ■

Proposição 2.2.3 *Se a e b são inteiros, então:*

(i) $a-b \mid a^n - b^n$, *quando* $a \neq b$;

(ii) $a+b \mid a^{2n} - b^{2n}$, *quando* $a \neq -b$.

Demonstração (i) Utilizaremos na demonstração o Princípio da Indução Matemática. A afirmação é verdade para $n = 1$. De fato,

$$a-b \mid a^1 - b^1 = a-b.$$

Suponhamos ser verdadeiro que $a-b \mid a^n - b^n$ para n inteiro positivo. Façamos:

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

Daí, como $a-b \mid a-b$ e por hipótese de indução $a-b \mid a^n - b^n$, decore que $a-b \mid a^{n+1} - b^{n+1}$. Portanto, $a-b \mid a^n - b^n$ para todo n inteiro positivo.

(ii) Novamente utilizaremos o Princípio de Indução Matemática. A afirmação é verdade para $n = 1$. De fato,

$$a+b \mid a^2 - b^2 = (a+b) \cdot (a-b).$$

Suponhamos que $a+b \mid a^{2n} - b^{2n}$ seja verdade para n inteiro positivo. Façamos:

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

Logo, como $a+b \mid a^2 - b^2$ e por hipótese de indução $a+b \mid a^{2n} - b^{2n}$ implica em $a+b \mid a^{2(n+1)} - b^{2(n+1)}$. Portanto, $a+b \mid a^{2n} - b^{2n}$ para todo n inteiro positivo. ■

O próximo resultado é devido ao matemático, astrônomo e filósofo grego Eudoxus (408-355 a.C.) nascido em Cnidos.

Eudoxus estudou com Arcquitas de Tarento, o mais conhecido e ilustre pitagórico. O problema de duplicar o cubo interessava a Arcquitas e é razoável supor que o interesse de Eudoxus por esse problema foi estimulado por seu professor. Outros tópicos prováveis que ele tenha aprendido, incluem a teoria dos números e a teoria da música. Eudoxus fez uma colaboração fundamental para a teoria da proporção, onde estabeleceu uma definição que permite os comprimentos possivelmente irracionais sejam comparados de forma semelhante ao método de multiplicação cruzada usado hoje. Uma grande dificuldade havia surgido na Matemática, o fato de que certos comprimentos não eram comparáveis. O método de comparação de dois comprimentos x e y encontrando um comprimento t

de modo que $x = m \cdot t$ e $y = n \cdot t$ para números inteiros m e n falhavam para linhas de comprimentos 1 e $\sqrt{2}$.

A teoria desenvolvida por Eudoxus está estabelecida no Livro V dos *Elementos* de Euclides, a Definição 4 nesse livro é chamada de axioma de Eudoxus e foi atribuída a ele por Arquimedes sendo assim anunciada:

Considera-se que as magnitudes têm uma proporção entre si que é capaz, quando um múltiplo de qualquer um pode exceder o outro.

Para Eudoxus significava que um comprimento e uma área não podiam ser comparadas. Mas uma linha de comprimento $\sqrt{2}$ e uma de comprimento 1 têm uma relação capaz desde que $1 \cdot \sqrt{2} > 1$ e $2 \cdot 1 > \sqrt{2}$. Por isso, o problema dos comprimentos irracionais foi resolvido no sentido de que se poderia comparar linhas de qualquer comprimento, seja racional ou irracional.

Teorema 2.2.3 (Eudoxus) *Se a e b inteiros com $b \neq 0$, então a é um múltiplo de b ou se encontra entre dois múltiplos consecutivos de b, isto é, existe um inteiro q tal*

(i) $b > 0 \Rightarrow qb \leq a < (q+1)b$;

(ii) $b < 0 \Rightarrow qb \leq a < (q-1)b$.

Demonstração Sejam $a > 0$ e $b > 0$ (os casos em que $a < 0$ ou $b < 0$ podem ser demonstrados de forma análoga).

(i) Se $a = qb$, para algum $q \in \mathbb{Z}$ nada a provar e o resultado segue.

(ii) Se $a \neq qb$ para todo $q \in \mathbb{Z}$ existe um menor inteiro k que satisfaz a condição $a < kb$. Podemos afirmar que

$$(k-1)b < a.$$

Se $a < (k-1)b$ contradiria o fato de $a < kb$ e k ser o menor inteiro para o qual isto ocorre. Assim devemos ter $(k-1)b < a$ e daí $(k-1)b < a < kb$. Tomando $q = k-1$ obtemos $qb \leq a < (q+1)b$. ∎

2.3 Algoritmo da Divisão de Euclides

Em Alexandria, Egito, surgiu por volta de 300 a.C. um tratado que se tornaria um dos marcos da Matemática, *Elementos* de Euclides. Neste tratado composto por treze livros (capítulos), encontram-se sistematizada a maior parte do conhecimento básico da Matemática da época.

Muitos resultados não são creditados a Euclides, mas ele teve o mérito de estabelecer um padrão de apresentação e rigor matemático jamais alcançado anteriormente,

tido como um exemplo a ser seguindo nos milênios que se sucederam. Dos treze livros de *Elementos*, dez versam sobre Geometria e três sobre Aritmética. Nos três livros de Aritmética, Livros VII, VIII e IX, Euclides desenvolve a teoria dos números naturais, sempre com uma visão geométrica. No Livro VII, são definidos os conceitos de divisibilidade, de número primo, de números perfeitos, de máximo divisor comum e de mínimo múltiplo comum, entre outros. No mesmo livro, encontra-se enunciada (sem demonstração) a divisão com resto de um número natural por outro, chamada divisão euclidiana. Após Euclides, a Aritmética estagnou por cerca de 500 anos, ressurgindo com os trabalhos de Diofanto de Alexandria que viveu por volta de 250 *d.C.*

Teorema 2.3.4 (Divisão Euclidiana) *Se a e b são inteiros positivos, com $b \neq 0$, então existe um único par de inteiros q e r tais que $a = qb + r$, com $0 \leq r < b$. Mais ainda, ocorre $r = 0$ se, e somente se, $b \mid a$.*

Demonstração *Existência*: Pelo teorema de Eudoxus, como $b > 0$ existe $q \in \mathbb{Z}$ tal que $qb \leq a < (q+1)b$, logo, $0 \leq a - qb < b$. Tomando $r = a - qb$, garante-se a existência de q e r.

Unicidade: Suponhamos a existência de um outro par q_1 e r_1 de forma que:

$$a = bq_1 + r_1 \text{ com } 0 \leq r_1 < b$$

Assim, temos $(bq + r) - (bq_1 + r_1) = 0$ implica que $b(q - q_1) = r_1 - r$ decorrendo que $b \mid r_1 - r$, logo, pela Proposição 2.2.1, p.12 implica em $b \mid |r_1 - r|$. Como $0 \leq r_1 < b$ e $0 \leq r < b$, temos $|r_1 - r| < b$, e assim como $b \mid |r_1 - r|$ teremos $r_1 - r = 0$, logo, $r_1 = r$ e assim temos $bq_1 = bq$, portanto, $q_1 = q$ já que $b \neq 0$. ∎

A próxima definição desempenha um papel fundamental na Aritmética.

Definição 2.3.3 (Número Primo) *Um número inteiro $(n > 1)$ possuindo somente dois divisores positivos n e 1 é chamado primo.*

Teorema 2.3.5 (Teorema Fundamental da Aritmética) *Todo número inteiro maior do que 1 ou é primo ou se escreve de modo único , a menos da ordem, como um produto de números primos.*

"A demonstração do teorema pode ser encontrada em [3, Teorema 1.9]."

Usaremos o Teorema Fundamental da Aritmética para provar que existe uma quantidade infinita de números primos.

Teorema 2.3.6 *A sequência dos números primos é infinita.*

Demonstração Provaremos o resultado pelo método de redução ao absurdo.

Consideremos finita a quantidade de números primos. Assim, podemos listar todos os números primos como $p_1, p_2, \ldots, p_n$. Seja R um número inteiro da forma $R = p_1 p_2 \ldots p_n + 1$. Como $R > p_i, i = 1, 2 \ldots n$, necessariamente R não é primo, logo possui algum fator primo p_i da nossa lista de números primos. Dessa forma, como $p_i \mid R$ e $p_i \mid p_1, p_2, \ldots, p_n$ implica que $p_i \mid R - p_1, p_2, \ldots, p_n$, ou seja, $p_i \mid 1$ o que é absurdo. Portanto a hipótese inicial é falsa. Logo, a quantidade de números primos é infinita. ■

2.4 Sistema de Numeração Decimal

O sistema de numeração decimal é construído utilizando dois conjuntos. Um alfabeto (conjunto) α constituído por dez letras (elementos) denominados dígitos ou algarismos, e outro conjunto β chamado base e constituído pelos números naturais que são potências de dez cujo registro é 10:

1. $\alpha = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\}$;
2. $\beta = \{1, 10, 10^2, 10^3, \ldots\}$.

Na construção das operações com naturais fica estabelecido a notoção: $10^0 = 1$; $10^1 = 10$.

Um número natural é registrado por uma palavra (numeral) escrita com as letras (algarismos) de α. Por exemplo, o numeral 1 representa o número natural que não é sucessor de nenhum outro, 2 é sucessor de 1, 3 é o sucessor de 2, etc. e 10 é o sucessor de 9. Aqui, definimos as operações $n + 0 = n$ e $n \cdot 0 = 0$, para todo número natural n. Definido o valor dos numerais com um algarismo, podemos definir o valor dos numerais com mais de um algarismo, observando a posição do algarismo no numeral, por isso o sistema é chamado de posicional. O numeral $x_n x_{n-1} \cdots x_1 x_0$ representa o número natural

$$x_n 10^n + x_{n-1} 10^{n-1} + \cdots + x_1 10 + x_0.$$

Como exemplo, observemos que o 13 018 é o registro de

$$1 \cdot 10^4 + 3 \cdot 10^3 + 0 \cdot 10^2 + 1 \cdot 10 + 8.$$

Para facilitar a comunicação, é estabelecido uma regra de leitura para um numeral. Cada algarismo possui uma ordem contada da direita para esquerda, de forma que, no exemplo acima, o primeiro um (1) que aparece é de segunda ordem enquanto que o três (3) é de quarta ordem. A cada terna de ordem forma-se uma classe.

(1) *Classe das Unidades* Compreendendo unidades, dezenas e centenas representando respectivamente a primeira, segunda e terceira ordens.

(2) *Classe do Milhar* Compreendendo unidades de milhar, dezenas de milhar e centenas de milhar representando respectivamente a quarta, quinta e sexta ordens.

(3) *Classe do Milhão* Compreendendo unidades de milhão, dezenas de milhão e centenas de milhão representando respectivamente a sétima, oitava e nona ordens.

Como aplicação do Algoritmo da Divisão de Euclides, Teorema 2.3.4, mostraremos o seguinte resultado.

Proposição 2.4.4 *Todo número inteiro positivo k pode ser escrito de forma única no sistema de numeração decimal.*

Demonstração (i) Vamos provar que k pode ser escrito na base decimal.

Pelo Algoritmo da Divisão de Euclides temos $k = q_0 10 + x_0$, com $0 \leq x_0 < 10$ em que $q_0 = x_n 10^{n-1} + x_{n-1} 10^{n-2} + \cdots + x_1$ e repetindo o processo indefinidamente vamos obter quocientes cada vez menores. Como o quociente não pode ser negativo ocorrerá um momento em que ele é nulo.
Supondo que quando tivermos o quociente nulo o resto será x_n, teremos:

$$\begin{aligned}
k &= q_0 10 + x_0, && 0 \leq x_0 < 10;\\
q_0 &= q_1 10 + x_1, && 0 \leq x_1 < 10;\\
q_1 &= q_2 10 + x_2, && 0 \leq x_2 < 10;\\
&\vdots\\
q_{n-2} &= q_{n-1} 10 + x_{n-1}, && 0 \leq x_{n-1} < 10;\\
q_{n-1} &= 0 \cdot 10 + x_n, && 0 \leq x_n < 10.
\end{aligned}$$

Substituindo q_0 na primeira expressão, q_1 na segunda expressão e assim por diante obteremos:

$$\begin{aligned}
k &= q_0 10 + x_0\\
&= 10(q_1 10 + x_1) + x_0\\
&= q_1 10^2 + x_1 10 + x_0\\
&= 10^2(q_2 10 + x_2) + x_1 10 + x_0\\
&\vdots\\
&= x_n 10^n + x_{n-1} 10^{n-1} + x_{n-2} 10^{n-2} + \cdots + x_1 10 + x_0.
\end{aligned}$$

Dessa forma mostramos que k pode ser escrito no sistema decimal.

(ii) Vamos provar que k se escreve de forma única.

Suponhamos que existem duas expressões para o número k, na mesma base 10 com $n \leq m$ e $x_n \neq 0$. Logo teríamos

$$k = x_n 10^n + x_{n-1}10^{n-1} + \cdots + x_1 10 + x_0 = y_m 10^m + y_{m-1}10^{m-1} + \cdots + y_1 10 + y_0,$$

com n, m naturais.
Tem-se que x_0 e y_0 são os restos da divisão de k por 10 e $x_n 10^{n-1} + x_{n-1}10^{n-2} + \cdots + x_1$ e $y_m 10^{m-1} + y_{m-1}10^{m-2} + \cdots + y_1$ seus respectivos quocientes. Assim pela unicidade do quociente e do resto temos,

$$x_0 = y_0 \text{ e } x_n 10^{n-1} + x_{n-1}10^{n-2} + \cdots + x_1 = y_m 10^{m-1} + y_{m-1}10^{m-2} + \cdots + y_1.$$

De forma análoga repetindo o processo obteríamos: $x_1 = y_1, x_2 = y_2, \cdots, x_n = y_m$ e $n = m$.

Portanto k se escreve de forma única. ■

2.5 Critérios de Divisibilidade

A seguir enunciaremos e demonstraremos os critérios de divisibilidade que são de boa comodidade para analisarmos quando um número é divisível ou não por outro. Isto facilita decompor um número natural em produto de potências de primos.

(1) **Critério de divisibilidade por** 2 *Um número é divisível por* 2 *se, e somente se, o algarismo das unidades é divisível por* 2.

(2) **Critério de divisibilidade por** 5 *Um número é divisível por* 5 *se, e somente se, o algarismo das unidades é divisível por* 5.

Demonstração Seja $k \in \mathbb{Z}$. Escrevendo k na forma decimal

$$\begin{aligned} k &= x_n 10^n + x_{n-1}10^{n-1} + x_{n-2}10^{n-2} + \cdots + x_2 10^2 + x_1 10 + x_0 \\ &= 10[x_n 10^{n-1} + x_{n-1}10^{n-2} + x_{n-2}10^{n-3} + \cdots + x_2 10 + x_1] + x_0 \\ &= 2 \cdot 5[x_n 10^{n-1} + x_{n-1}10^{n-2} + x_{n-2}10^{n-3} + \cdots + x_2 10 + x_1] + x_0. \end{aligned}$$

Tomando $q = 5[x_n 10^{n-1} + x_{n-1}10^{n-2} + x_{n-2}10^{n-3} + \cdots + x_2 10 + x_1]$ temos

$$k = 2q + x_0.$$

Portanto $2 \mid k$ se, e somente se, $2 \mid x_0$.

De forma análoga para o critério por 5 basta fazermos

$$q' = 2[x_n 10^{n-1} + x_{n-1}10^{n-2} + x_{n-2}10^{n-3} + \cdots + x_2 10 + x_1]$$

e teremos

$$k = 5q' + x_0.$$

Portanto $5 \mid k$ se, e somente se, $5 \mid x_0$. ■

(3) **Critério de divisibilidade por** 3. *Um número é divisível por* 3*, se somente se, a soma de seus dígitos é divisível por* 3*.*

Demonstração Primeiro mostremos que $(10^n - 1)$ é um múltiplo de 9.

Como $(10^n - 1) = 10^n - 1^n$, pelo item (i) da Proposição 2.2.3, p.13 temos $(a-b) \mid (a^n - b^n)$. Logo $(10-1) \mid (10^n - 1)$ o que implica que $(10^n - 1) = 9p$. Seja

$$k = x_n 10^n + x_{n-1}10^{n-1} + x_{n-2}10^{n-2} + \cdots + x_2 10^2 + x_1 10 + x_0.$$

Escrevendo k da seguinte forma:

$$\begin{aligned} k &= x_n(10^n - 1 + 1) + x_{n-1}(10^{n-1} - 1 + 1) + \cdots + x_1(10 - 1 + 1) + x_0 \\ &= x_n(10^n - 1) + x_{n-1}(10^{n-1} - 1) + \cdots + x_1(10 - 1) + (x_n + x_{n-1} + \cdots + x_1 + x_0). \end{aligned}$$

Utilizando o fato de $(10^n - 1)$ ser um múltiplo de 9 temos:

$$\begin{aligned} k &= (9p_n)x_n + (9p_{n-1})x_{n-1} + \cdots + 9x_1 + (x_n + x_{n-1} + \cdots + x_1 + x_0) \\ &= 3 \cdot [3(p_n)x_n + 3(p_{n-1})x_{n-1} + \cdots + 3x_1] + (x_n + x_{n-1} + \cdots + x_1 + x_0). \end{aligned}$$

Tomando $m = [3(p_n)x_n + 3(p_{n-1})x_{n-1} + \cdots + 3x_1]$ e $q = (x_n + x_{n-1} + \cdots + x_1 + x_0)$ temos,

$$k = 3m + q.$$

Portanto $3 \mid k$ se, somente se, $3 \mid q$. ■

(4) **Critério de divisibilidade por** 9. *Um número é divisível por* 9*, se somente se, a soma de seus dígitos é divisível por* 9*.*

Demonstração Utilizando a construção feita na demonstração anterior e tomando

$$k = 9[(p_n)x_n + (p_{n-1})x_{n-1} + \cdots + x_1] + (x_n + x_{n-1} + \cdots + x_1 + x_0).$$

Fazendo $m = [(p_n)x_n + (p_{n-1})x_{n-1} + \cdots + x_1]$ e $q = (x_n + x_{n-1} + \cdots + x_1 + x_0)$ temos

$$k = 9m + q.$$

Portanto $9 \mid k$ se, e somente se, $9 \mid q$. ■

(5) **Critério de divisibilidade por** 4 *Um número será divisível por* 4 *se, e somente se, o número formado pelos dois últimos dígitos forem divisíveis por* 4.

Demonstração Seja $k = x_n 10^n + x_{n-1}10^{n-1} + x_{n-2}10^{n-2} + ... + x_2 10^2 + x_1 10 + x_0$. Escrevendo

$$k = 100 \cdot [x_n 10^{n-2} + x_{n-1}10^{n-3} + ... + x_2] + x_1 10 + x_0.$$

Tomando $10x_1 + x_0 = m$ teremos:

$$\begin{aligned} k &= 100 \cdot [x_n 10^{n-2} + x_{n-1}10^{n-3} + ... + x_2] + m \\ &= 4 \cdot 25[x_n 10^{n-2} + x_{n-1}10^{n-3} + ... + x_2] + m. \end{aligned}$$

Fazendo $q = 25[x_n 10^{n-2} + x_{n-1}10^{n-3} + ... + x_2]$ temos

$$k = 4q + m.$$

Portnto $4 \mid k$ se, e somente se, $4 \mid m$ com $0 \leq m < 100$ o resultado segue. ■

(6) **Critério de divisibilidade por 7** *Um número* $k = x_n x_{n-1} \ldots x_1 x_0$ *é divisível por* 7 *se, e somente se, o número formado pela diferença entre o número obtido de* k *retirendo-se o algarismo das unidades e o dobro do algarismo das unidades é divisível por* 7.

O exemplo que segue servirá para entendimento do critério e auxílio do processo demonstrativo.

Exemplo 2.5.1 Considere o número $k = 69720$. Inicialmente separamos o dígito 0 da unidade e do número restante 6972 subtraímos o dobro deste dígito, ou seja

$$6972 - 0 = 6972.$$

A seguir repetimos o processo até obtemos um número suficientemente pequeno de forma que possamos, reconhecer, rapidamente se é ou não divisível por 7.

$$697 - 4 = 693.$$
$$69 - 6 = 63.$$

Como 63 é divisível por 7 o que iremos demonstrar é que tal fato implica ser o número original também divisível por 7.

Demonstração Seja k um número da forma $k = 10 \cdot [x_n 10^{n-1} + ... + x_2 10^2 + x_1] + x_0$.
Simplificando a notação temos

$$q = 10 \cdot [x_n 10^{n-1} + ... + x_2 10 + x_1], \text{ tem-se } k = 10q + x_0.$$

Seja o número $r = q - 2x_0$. . Vamos mostrar que

$$7 \mid k \Leftrightarrow 7 \mid r.$$

(i) Se $7 \mid k$ implica que $7 \mid 10q + x_0$, então existe um inteiro p tal que $10q + x_0 = 7p$, daí $x_0 = 7p - 10q$.

Logo,

$$\begin{aligned} q - 2x_0 &= q - 2(7p - 10q) \\ &= q - 14p + 20q \\ &= 7(3q - 2p). \end{aligned}$$

Assim $q - 2x_0 = 7u$, com $u \in \mathbb{Z}$. Portanto, $7 \mid r$.

(ii) Se $7 \mid r$ implica que $7 \mid q - 2x_0$, então existe um inteiro n tal que $q - 2x_0 = 7n$, daí $q = 7n + 2x_0$.

Logo,

$$\begin{aligned} 10q + x_0 &= 10(7n + 2x_0) + x_0 = 70n + 20x_0 + x_0. \\ &= 70n + 21x_0 = 7(10n + 3x_0). \end{aligned}$$

Assim $10q + x_0 = 7v$, com $v \in \mathbb{Z}$. Portanto, $7 \mid k$.

■

(7) **Critério de divisibilidade por** 11. *Um número natural* $k = x_n x_{n-1} \dots x_1 x_0$ *é divisível por* 11 *se, e somente se, a soma alternada dos seus algarismos* $x_0 - x_1 + x_2 - \cdots + (-1)^n x_n$ *for um número divisível por* 11.

Lema 2.5.1 *Para todo* n *natural com* $n \geq 1$, *tem-se que* $10^n = 11q + (-1)^n$.

Demonstração Usando o Princípio da Indução Matemática sobre n a afirmação é verdade para $n = 1$. De fato, $10 = 11 - 1$.
Suponhamos ser verdadeiro que $10^n = 11q + (-1)^n$ para algum n natural e façamos

$$10^{n+1} = 10^n \cdot 10.$$

Sendo assim, $10^{n+1} = [11q + (-1)^n] \cdot 10$ por hipótese de indução. Logo

$$\begin{aligned} 10^{n+1} &= 11 \cdot 10q + 10 \cdot (-1)^n \\ &= 11 \cdot 10q + (11-1) \cdot (-1)^n \\ &= 11 \cdot 10q + 11 \cdot (-1)^n + (-1) \cdot (-1)^n \\ &= 11 \cdot [10q + (-1)^n] + (-1)^{n+1}. \end{aligned}$$

Tomando $q' = [10q + (-1)^n]$ temos

$$10^{n+1} = 11q' + (-1)^{n+1}.$$

Logo é verdade que $10^n = 11q + (-1)^n$ para todo n natural. ■

Provemos agora o critério de divisibilidade por 11 acima citado.

Seja $k = x_n 10^n + x_{n-1} 10^{n-1} + ... + x_2 10^2 + x_1 10 + x_0$ com $0 \leq x_i \leq 9$.
Usando o Lema 2.5.1 podemos escrever:

$$\begin{aligned} k &= x_n[11q_n + (-1)^n] + \cdots + x_2[11q_2 + (-1)^2] + x_1[11q_1 + (-1)] + x_0 \\ &= 11 \cdot (x_n q_n + \cdots + x_2 q_2 + x_1 q_1) + (x_0 - x_1 + x_2 - \cdots + (-1)^n x_n). \end{aligned}$$

Tomando $m = (x_n q_n + \cdots + x_2 q_2 + x_1 q_1)$ e $p = (x_0 - x_1 + x_2 - \cdots + (-1)^n x_n)$ temos

$$k = 11m + p.$$

Portanto $11 \mid k$ se, e somente se, $11 \mid p$.

(8) **Construção de um critério.**

Seja $p = abcd$ um natural. Iniciemos com uma observação: $p - d$ é divisível por 10.

Definindo o natural

$$q = \frac{p-d}{10} - 2d.$$

Explicitando o valor de p temos

$$p = 10q + 21d.$$

Portanto, p é divisível por 7, se, e somente se, q for divisível por 7.

O critério de divisibilidade por 7 apresentado acima pode ser generalizado . Seja $p = abcd$ um natural. Como vimos, $q = p - d$ é divisível por 10. Seja λ um natural qualquer. Considere o natural

$$q = \frac{p-d}{10} - \lambda d.$$

Explicitando o valor de p temos

$$p = 10q + (10\lambda + 1)d.$$

Com essa construção podemos determinar vários critérios de divisibilidade. Por exemplo, para $\lambda = 1$ temos o critério por 11.

Observação 2.5.1 Há dois fatos interessantes sobre divisibilidade por 11.

(i) Todo número na forma 999...9 onde o número do dígito é par é divisível por 11.
Basta verificar que $9999 = 9900 + 99$, $999999 = 999900 + 99$ ou aplicar o critério de divisibilidade $9 - 9 + 9 - 9 = 0$.

(ii) Todo número da forma 100...01, onde o dígito $''0''$ entre dois $''uns''$ é par é múltiplo de 11.
Basta verificar que $1001 = 990 + 11$, $100001 = 99990 + 11$ ou aplicar o critério de divisibilidade $1 - 0 + 0 - 1$.

2.6 Outros Sistemas de Numeração

A construção de um sistema de numeração diferente do sistema decimal segue os mesmos procedimentos. Escolhido um natural b, o sistema de numeração na base b é construído utilizando dois conjuntos. Um alfabeto (conjunto) α constituído por dez letras (elementos) denominados dígitos ou algarismos, e outro conjunto β chamado base e constituído pelos naturais que são potências de b:

1. $\alpha = \{x_1, x_2, x_3, \ldots, x_{b-1}, x_b\}$;
2. $\beta = \{1, b, b^2, b^3, \ldots\}$.

Usualmente $x_b = 0$, e as operações de adição e multiplicação por 0 segue a regra habitual. Um número natural é registrado por uma palavra (numeral) escrita com as letras (algarismos) de α. O numeral x_1 representa o número natural que não é sucessor de nenhum outro, x_2 é o sucessor de x_1, x_3 é o sucessor de x_2, etc. Definido o valor dos numerais com um algarismo, podemos definir o valor dos numerais com mais de um algarismo, observando a posição do algarismo no numeral, por isso o sistema é chamado de posicional. O numeral $x_{i_n} \ldots x_{i_1} x_{i_0}$ representa o numero natural

$$x_{i_n} b^n + \cdots + x_{i_1} b + x_{i_0}.$$

No caso em que a base é maior que 10 como a representação dos algarismo vai de $0, 1, 3, \cdots, 9$ devemos acrescentar novos símbolos a coleção. Por exemplo, sendo $b = 13$, temos $D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \lambda, \phi, \omega\}$ com λ, ϕ e ω, respectivamente, os representantes do 10, 11 e 12. Logo, $[36\lambda 7\omega]_{13}$ tem como registro

$$3 \cdot 13^4 + 6 \cdot 13^3 + 10 \cdot 13^2 + 7 \cdot 13 + 12,$$

cuja representação decimal é o número 100 658.

A seguir mostraremos como passar o número inteiro positivo k da base decimal para uma base b. Escrevendo k na base decimal temos

$$k = x_n 10^n + x_{n-1} 10^{n-1} + \cdots + x_2 10^2 + x_1 10 + x_0, \tag{2.1}$$

com $0 \leq x_i < 10$. Devemos determinar os inteiros $y_n, y_{n-1}, \ldots, y_0$ na expressão

$$k = y_n b^n + y_{n-1} b^{n-1} + \cdots + y_2 b^2 + y_1 b + y_0,$$

com $0 \leq y_i < b$. Divindo a equação (2.1) por b obtemos

$$\begin{aligned} K/b &= x_n 10^n/b + x_{n-1} 10^{n-1}/b + \cdots + x_2 10^2/b + x_1 10/b + x_0/b \\ &= K' + x_0/b. \end{aligned}$$

Assim o resto x_0 dessa divisão é o último algarismo y_0 da representação desejada. Dividindo-se K' por b obtemos

$$k'/b = x_n 10^n/b^2 + x_{n-1} 10^{n-1}/b^2 + \cdots + x_2 10^2/b^2 + x_1 10/b^2$$

e o resto dessa divisão é o penúltimo algarismo y_1 da representação desejada. Continuando o procedimento obteremos todos os dígitos $y_n, y_{n-1}, \ldots, y_0$.

Exemplo 2.6.2 Escrevamos 783 na base 6.

$$\begin{aligned} 783 &= 130 \cdot 6 + 3 \\ 130 &= 21 \cdot 6 + 4 \\ 21 &= 3 \cdot 6 + 3 \\ 3 &= 0 \cdot 6 + 3 \end{aligned}$$

Logo $783 = 3 \cdot 6^3 + 3 \cdot 6^2 + 4 \cdot 6 + 3$ e portanto $783 = [3343]_6$

Exemplo 2.6.3 Escrevamos 5483 na base 13.

$$\begin{aligned} 5483 &= 421 \cdot 13 + 10 \\ 421 &= 32 \cdot 13 + 5 \\ 32 &= 2 \cdot 13 + 6 \\ 2 &= 0 \cdot 13 + 2 \end{aligned}$$

Daí $5483 = 2 \cdot 13^3 + 6 \cdot 13^2 + 5 \cdot 13 + 10$.

Assim devemos acrescentar um novo símbolo para representar o 10. Denotemos este símbolo por λ. Portanto $5483 = [265\lambda]_{13}$.

Usando tábuas correspondentes construídas para uma base b podemos igualmente efetuar adições e multiplicações no novo sistema sem, em momento nenhum, ter que fazer a transformação para o sistema decimal.

Vamos ilustrar esse fato com a base 6 e construiremos as tábuas de adição e multiplicação correpondentes.

Adição

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	10
2	2	3	4	5	10	11
3	3	4	5	10	11	12
4	4	5	10	11	12	13
5	5	10	11	12	13	14

Multiplicação

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	10	12	14
3	0	3	10	13	20	23
4	0	4	12	20	24	32
5	0	5	14	23	32	41

Exemplo 2.6.4 Multipliquemos $[204]_6$ por $[25]_6$.

$$\begin{array}{rcccc} & & 2 & 0 & 4 \\ & & \times & 2 & 5 \\ \hline & 1 & 4 & 3 & 2 \\ + & 4 & 1 & 2 & \\ \hline & 5 & 5 & 5 & 2 \end{array}$$

As operações foram realizadas com o auxílio das tabuadas acima. ◇

3 CONGRUÊNCIAS

Carl Friederich Gauss(1777-1855) foi um dos maiores matemáticos de todos os tempos

Gaus nasceu em Brunswick, Alemanha, filho de uma modesta família e manifestou o seu gênio na mais tenra idade, aprendendo a ler sozinho e demonstrando uma habilidade ímpar em realizar complicados cálculos mentais. Em 1798, aos 21 anos, Gaus produz uma das obras primas da matemática, o livro *Disquisitiones Arithmeticae*, que seria publicado somente 1801. No livro, Gaus introduz a noção de congruência, desenvolve a teoria dos resíduos quadráticos, demonstrando a profunda *Lei da Reciprocidade Quadrática.*

Em Matemática Pura deu contribuições à teoria das probabilidades e foi um dos criadores das geometrias não-euclidianas, da geometria diferencial, das funções de variável complexa e da Teoria Algébrica dos Números. Gaus teve o poder de mudar os rumos da Matemática a partir dos seus trabalhos revolucionários, apresentados com rigor, concisão e elegância

3.1 Propriedades de Congruência

Citamos [1] como referência para esta seção.

Definição 3.1.4 *Sejam a, b e m inteiros com $m > 0$. Diz-se que a é congruente a b módulo m se $m \mid a - b$.*

Denotaremos a condição "a é congruente a b módulo m" pelo símbolo $a \equiv b \; mod \; m$. Caso m não divida $a - b$, fato indicado por $m \nmid a - b$, diremos que a é incongruente a b módulo m e denotaremos por $a \not\equiv b \; mod \; m$.

Exemplo 3.1.5 $12 \equiv 5 \; mod \; 7$, $7 \mid 12 - 5$. Já $13 \not\equiv 6 \; mod \; 5$, $5 \nmid 13 - 5$. ◇

Vejamos uma proposição que será utilizada posteriormente.

Proposição 3.1.5 *Seja a e b inteiros, tem-se $a \equiv b \; mod \; m$ se, somente se, existir um inteiro p tal que $a = b + pm$.*

Demonstração ($\Rightarrow$) Se $a \equiv b \; mod \; m$, por definição $m \mid a - b$, daí existe p inteiro tal que $a - b = pm$, ou seja, $a = b + pm$.

($\Leftarrow$) Do fato da existência de um inteiro p e que $a - b = pm$ decorre que $m \mid a - b$. Logo $a \equiv b \; mod \; m$. ■

Algumas observações sobre a relação entre restos de divisões e congruência serão centrais para o desenvolvimento do texto.

Proposição 3.1.6 *Sejam a, b e $m > 0$ inteiros. As seguintes afirmações são verdadeiras.*

(*i*) *$a \equiv b \bmod m$ se, e somente se, o resto da divisão de a por m e o resto da divisão de b por m são iguais.*

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

Demonstração Escrevamos $a = pm + r$ e $b = qm + r'$ com $0 \leq r, r' < m$. Sem perda de generalidade, podemos assumir que $r' \leq r$. Sendo assim, $0 \leq r - r' < m$, portanto $r - r' = 0m + (r - r')$.

(*i*) Temos, $a \equiv b \bmod m$ se, e somente se $m|a - b$, ou equivalentemente, $m|(p-q)m + r - r'$. Como $m|(p-q)m$, a penúltima divisão ocorre se, e somente se, $m|r - r'$ com $0 \leq r - r' < m$. Ou seja, $a \equiv b \bmod m$ se, e somente se, $r = r'$.

(*ii*) Se $a = pm + r$ com $0 \leq r < m$. Logo, $a - r = pm$, ou equivalentemente $a \equiv r \bmod m$. Reciprocamente, se $a \equiv r \bmod m$ com $0 \leq r < m$, pela Proposição 3.1.5 desta seção, $a = pm + r$. Como o resto da divisão de a por m é único, segue que r é o resto. ■

A congruência é uma relação de equivalência, ou seja, é: *reflexiva; simétrica; transitiva*. Mostremos estas propriedades.

Proposição 3.1.7 *Sejam a, b, c e d inteiros e m um inteiro positivo. As seguintes afirmações são verdadeiras.*

(*i*) $a \equiv a \bmod m$. *Reflexiva*

(*ii*) Se $a \equiv b \bmod m$, então $b \equiv a \bmod m$. *Simétrica*

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

Demonstração (*i*) Como $m \mid 0$, segue que $m \mid a - a$ implicando assim que $a \equiv a \bmod m$.

(*ii*) Se $a \equiv b \bmod m$, então existe um inteiro p de modo que $a = b + pm$. Daí $b = a - pm$ e logo $b \equiv a \bmod m$.

(*iii*) Se $a \equiv b \bmod m$ e se $b \equiv c \bmod m$, então existem p_1 e p_2 inteiros tais que $a - b = p_1 m$ e $b - c = p_2 m$, somando-se as equações membro a membro obtemos $a - c = (p_1 + p_2)m$, ou seja, $m \mid a - c$. Portanto $a \equiv c \bmod m$. ■

Tendo em vista a proposição anterior, podemos particionar o conjunto dos inteiros $\mathbb{Z}$ em m conjuntos disjuntos, chamados classes residuais. Como o resto da divisão de um inteiro por m é um único inteiro r, com $0 \leq r \leq m-1$, definimos os conjuntos, denotado por $\overline{r}$ constituído pelos inteiros cujos restos da divisão por m é r

$$\begin{aligned}
\overline{0} &= \{0, \pm m, \pm 2m, \pm 3m, \dots\} \\
\overline{1} &= \{1, 1 \pm m, 1 \pm 2m, 1 \pm 3m, \dots\} \\
&\dots \\
\overline{r} &= \{r, r \pm m, r \pm 2m, r \pm 3m, \dots\} \\
&\dots \\
\overline{m-1} &= \{(m-1), (m-1) \pm m, (m-1) \pm 2m, (m-1) \pm 3m, \dots\}
\end{aligned}$$

Uma outro modo de definir estes conjuntos pode ser $\overline{r} = \{a \in \mathbb{Z};\ a \equiv r\ mod\ m\}$. Claro,

$$\mathbb{Z} = \bigcup_{r=1}^{m-1}{}^{\cdot}\ \overline{r}.$$

O símbolo $\cup$ sinaliza que os conjunto são disjuntos.

Denotaremos por $\mathbb{Z}_m$ o conjunto das classes residuais, mais precisamente,

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \dots, \overline{r}, \dots, \overline{m-1}\}.$$

O noves fora tem como justificativa as propriedades do conjunto $\mathbb{Z}_9$, que, por definição, é o conjunto constituído pelas classes de resíduos de 9:

$$\mathbb{Z}_9 = \{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5},\ \overline{6},\ \overline{7},\ \overline{8}\}.$$

Uma notação útil para redação é utilizar outras indicações para uma mesma classe de resíduo. Um elemento $\overline{r} \in \mathbb{Z}_m$ será representado também por $\overline{a}$ para qualquer elemento de $a \in \overline{r}$, ou seja, esta notação nos permite escrever $\overline{a} = \overline{r}$ pois o resto da divisão de a por m é r.

Exemplo 3.1.6 Em $\mathbb{Z}_9$ podemos escrever $\overline{4} = \overline{13} = \overline{31}$ pois 13 e 31 têm como restos da divisão por 9 o mesmo valor 4. ◇

Em resumo, para um inteiro $m > 0$, tirar o m's fora de um inteiro a é calcular a classe de resíduo de $\mathbb{Z}_m$ a qual a pertence, ou seja, calcular o resto da divisão de a por m, classe de resíduo este indicado por $\overline{a} \in \mathbb{Z}_m$.

Para continuar precisamos construir uma "aritmética" no conjunto $\mathbb{Z}_m$, ou seja, definir duas operações, uma adição e uma multiplicação entre os elementos de $\mathbb{Z}_m$. Este é o assunto da próxima seção.

3.2 Aritmética de $\mathbb{Z}_m$

Para definir uma soma em $\mathbb{Z}_m$ precisamos de um lema.

Lema 3.2.2 *Sejam $\overline{r}, \overline{s} \in \mathbb{Z}_m$. Se $a, b \in \overline{r}$ e $c, d \in \overline{s}$, então $a+c \equiv b+d \bmod m$. Em particular, $a+c$ e $b+d$ pertencem à mesma classe de resíduo de m, qual seja $\overline{r+s}$.*

Demonstração Pelas hipóteses podemos escrever:

$$\begin{cases} a = p_1 m + r \\ c = q_1 m + s \end{cases}; \qquad \begin{cases} b = p_2 m + r \\ d = q_2 m + s \end{cases}.$$

Por adição obtemos:

$$a + c = (p_1 + q_1)m + r + s; \qquad b + d = (p_2 + q_2)m + r + s.$$

Portanto, o resto da divisão de $a+c$ por m e o resto da divisão $b+d$ por m é o resto da divisão de $r+s$ por m. Como os retos são iguais, pela item (i) da Proposição 3.1.6, p. 27, segue que $a+c \equiv b+d \; mod \; m$. Em particular, $a+c$ e $b+d$ pertence à classe de resíduo de $r+s$. ∎

Definição 3.2.5 *Sejam $\overline{a}, \overline{b} \in \mathbb{Z}_m$. Definimos $\overline{a} + \overline{b} =: \overline{a+b}$.*

Nesta definição, o sinal + à esquerda diz respeito à operação com elementos de $\mathbb{Z}_m$ enquanto o sinal + à direita envolve elementos de $\mathbb{Z}$. O lema acima garante que a soma está bem definida, não depende do representante escolhido para representar a classe de resíduo. Vejamos. Se $\overline{a} = \overline{b}$ e $\overline{c} = \overline{d}$, então

$$\overline{a} + \overline{c} =: \overline{a+c} = \overline{b+d} =: \overline{b} + \overline{d}.$$

Observe que, para a soma, vale a lei do cancelamento. Se $\overline{a} + \overline{c} = \overline{b} + \overline{c}$, então $\overline{a} = \overline{b}$.

Exemplo 3.2.7 Consideremos $\overline{2}, \overline{4} \in \mathbb{Z}_5$. Como sabemos

$$\overline{2} = \{2,\, 2 \pm 5,\, 2 \pm 10,\, 2 \pm 15, \dots\} \quad \text{e} \quad \overline{4} = \{4,\, 4 \pm 5,\, 4 \pm 10,\, 4 \pm 15, \dots\}.$$

Pela definição, $\overline{2} + \overline{4} = \overline{2+4} = \overline{1}$. Esta operação poderia ser feita com qualquer representante. Por exemplo, seja $2 + 15 \in \overline{2}$ e $4 + 10 \in \overline{4}$. Avaliemos: $(2 + 15) + (4 + 10) = 6 + 25$. Calculando o resto da divisão por 5, temos $\overline{6+25} = \overline{1}$. ◇

A adição em $\mathbb{Z}_m$ possui as propriedades usuais da adição. Recordamos que $\overline{m} = \overline{0}$.

Proposição 3.2.8 *Sejam $\overline{a}$, $\overline{b}$ e $\overline{c}$ elementos de $\mathbb{Z}_m$. A adição possui as seguintes propriedades.*

(i) $\overline{a}+\overline{b}=\overline{b}+\overline{a}$. *(comutativa)*

(ii) $\overline{0}+\overline{a}=\overline{a}=\overline{a}+\overline{0}$. *(elemento neutro aditivo)*

(iii) $\overline{a}+\overline{-a}=\overline{0}$. *(elemento inverso aditivo)*

(iv) $(\overline{a}+\overline{b})+\overline{c}=\overline{a}+(\overline{b}+\overline{c})$. *(associatividade)*

Demonstração Pela Definição 3.2.5, temos

$$\begin{cases} (i)\ \ \overline{a}+\overline{b}=:\overline{a+b}=\overline{b+a}=\overline{b}+\overline{a}. \\ (ii)\ \ \overline{0}+\overline{a}=:\overline{0+a}=\overline{a}=\overline{a+0}=\overline{a}+\overline{0}. \\ (iii)\ \ \overline{a}+\overline{-a}=:\overline{a-a}=\overline{0}. \\ (iv)\ \ (\overline{a}+\overline{b})+\overline{c}=\overline{a+b}+\overline{c}=:\overline{(a+b)+c}=\overline{a+(b+c)}=\overline{a}+\overline{b+c}=\overline{a}+(\overline{b}+\overline{c}). \end{cases}$$

■

O inverso aditivo acompanha a notação usual, $\overline{-a}=-\overline{a}$.

Apresentemos a tabuada de soma de $\mathbb{Z}_9$. Pelo visto, podemos considerar representante especiais das classes de resíduos: $\{\overline{0},\overline{1},\ \overline{2},\overline{3},\overline{4},\overline{5},\overline{6},\overline{7},\overline{8}\}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{7}$	$\overline{7}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{8}$	$\overline{8}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$

Para ilustrar a tabuada de adição em $\mathbb{Z}_9$ é como segue. Por exemplo, $\overline{7}+\overline{8}$ é o resto da divisão de $7+8=15$ por 9, portanto, $\overline{7}+\overline{8}=\overline{6}$.

Para definir a multiplicação em $\mathbb{Z}_m$ necessitamos também de um lema auxiliar.

Lema 3.2.3 *Sejam $\overline{r}, \overline{s} \in \mathbb{Z}_m$. Se $a, b \in \overline{r}$ e $c, d \in \overline{s}$, então $ac \equiv bd \bmod m$. Em particular, ac e bd pertencem à mesma classe de resíduo de m, qual seja $\overline{rs}$.*

Demonstração Pelas hipóteses podemos escrever:

$$\begin{cases} a = p_1 m + r \\ c = q_1 m + s \end{cases}; \qquad \begin{cases} b = p_2 m + r \\ d = q_2 m + s \end{cases}.$$

Por multiplicação obtemos:

$$ac = (p_1 q_1 m + r + s)m + rs; \qquad bd = (p_2 q_2 m + r + s)m + rs.$$

Portanto, o resto da divisão de ac por m e o resto da divisão bd por m é o resto da divisão de rs por m. Como os retos são iguais, pela item (i) da Proposição 3.1.6, p. 27, segue que $ac \equiv bd \bmod m$. Em particular, ac e bd pertence à classe de resíduo $\overline{rs}$. ■

Definição 3.2.6 *Sejam $\overline{a}, \overline{c} \in \mathbb{Z}_m$. Definimos $\overline{a} \cdot \overline{c} =: \overline{ac}$.*

O lema garante que a multiplicação está bem definida, não depende do elemento escolhido para representar a classe de resíduo. Vejamos. Se $\overline{a} = \overline{b}$ e $\overline{c} = \overline{d}$, então

$$\overline{a} \cdot \overline{c} =: \overline{ac} = \overline{bd} =: \overline{b} \cdot \overline{d}.$$

Apresentemos a seguir a tabuada de multiplicação em $\mathbb{Z}_9$.

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{0}$	$\overline{3}$	$\overline{6}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{3}$	$\overline{7}$	$\overline{2}$	$\overline{6}$	$\overline{1}$	$\overline{5}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{1}$	$\overline{6}$	$\overline{2}$	$\overline{7}$	$\overline{3}$	$\overline{8}$	$\overline{4}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{6}$	$\overline{3}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Para ilustrar, a tabuada de multiplicação em $\mathbb{Z}_9$ observemos a regra. Por exemplo, $\overline{3} \cdot \overline{4}$ é o resto da divisão de $3 \cdot 4 = 12$ por 9, portanto, $\overline{3} \cdot \overline{4} = \overline{3}$.

Um fato a ressaltar na tabela acima é que algumas classes de resíduo não possuem o inverso multiplicativo enquanto outros possuem. É o caso de $\overline{3}$ que não tem inverso multiplicativo, mas $\overline{5}$ tem como inverso multiplicativo $\overline{2}$.

A operação de multiplicação em $\mathbb{Z}_m$ possui as seguintes propriedades.

Proposição 3.2.9 *Sejam $\overline{a}$, $\overline{b}$ e $\overline{c}$ elementos de $\mathbb{Z}_m$. A multiplicação possui as seguintes propriedades.*

(i) $\overline{a}\cdot\overline{b} = \overline{b}\cdot\overline{a}$. *(comutativa)*

(ii) $\overline{1}\cdot\overline{a} = \overline{a} = \overline{a}\cdot\overline{1}$. *(elemento neutro multiplicativo)*

(iii) $(\overline{a}\cdot\overline{b})\cdot\overline{c} = \overline{a}\cdot(\overline{b}\cdot\overline{c})$. *(associatividade)*

Demonstração Pela Definição 3.2.6, temos

$$\begin{cases} (i)\ \ \overline{a}\cdot\overline{b} =: \overline{a\times b} = \overline{b\times a} = \overline{b}\cdot\overline{a}. \\ (ii)\ \ \overline{1}\cdot\overline{a} =: \overline{1\times a} = \overline{a} = \overline{a}\cdot\overline{1}. \\ (iii)\ \ (\overline{a}\cdot\overline{b})\cdot\overline{c} = \overline{a\times b}\cdot\overline{c} =: \overline{(a\times b)\times c} = \overline{a\times(b\times c)} = \overline{a}\cdot\overline{b\times c} = \overline{a}\cdot(\overline{b}\cdot\overline{c}). \end{cases}$$

■

A relação entre o produto e a soma é a usual da Aritmética dos inteiros, vale a distributividade.

Proposição 3.2.10 *Se $\overline{a}$, $\overline{b}$ e $\overline{c}$ são elementos de $\mathbb{Z}_m$, então $\overline{a}\cdot(\overline{b}+\overline{c}) = \overline{a}\cdot\overline{b} + \overline{a}\cdot\overline{c}$.*

Demonstração Usando as Definições 3.2.5 e 3.2.6, temos

$$\overline{a}\cdot(\overline{b}+\overline{c}) = \overline{a}\cdot\overline{b+c} =: \overline{a\times(b+c)} = \overline{ab+ac} = \overline{ab} + \overline{ac} = \overline{a}\cdot\overline{b} + \overline{a}\cdot\overline{c}.$$

■

O conjunto $\mathbb{Z}_m$ equipado com as duas operações + e $\cdot$ é denominado anel dos inteiros módulo m.

Proposição 3.2.11 *Se a, b, n e m são inteiros com $n > 0$ e $a \equiv b \bmod m$ então $a^n \equiv b^n \bmod m$*

Demonstração A demonstração segue por indução sobre n.

Para n = 1 a afirmação é verdade pois $a^1 \equiv b^1 \bmod m$ implica $a \equiv b \bmod m$.

Suponhamos ser verdade que $a^n \equiv b^n \bmod m$ para n inteiro, com $n > 0$. Sendo assim, temos

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

Como $m \mid a-b$ e por hipótese de indução $m \mid (a^n - b^n)$ implica que $m \mid a^{n+1} - b^{n+1}$ e logo $a^{n+1} \equiv b^{n+1} \bmod m$. Portanto $a^n \equiv b^n \bmod m$ para todo n inteiro, com $n > 0$. ■

3.3 Aritmética de $\mathbb{Z}_p$, p primo

Definição 3.3.7 *Um elemento $\overline{a} \in \mathbb{Z}_m$ é dito invertível, se existir $\overline{b} \in \mathbb{Z}_m$, tal que $\overline{a} \cdot \overline{b} = \overline{1}$. Caso isto ocorra, chamamos $\overline{b}$ de inverso multiplicativo de $\overline{a}$.*

Como vimos na tabela de multiplicação de $\mathbb{Z}_9$, ver p. 31, a classe de resíduo $\overline{3}$ tem um comportamento diferenciado. A multiplicação desta classe de resíduo por algumas outras classes pode ser igual a $\overline{0}$ sem que elas sejam iguais à classe de resíduo zero,

$$\overline{0} = \overline{3} \cdot \overline{0} = \overline{3} \cdot \overline{3} = \overline{3} \cdot \overline{6}.$$

Essencialmente isto decorre da decomposição de 9 em fatores primos, qual seja $9 = 3 \cdot 3$. Logo, $\overline{0} = \overline{9} = \overline{3} \cdot \overline{3}$. Mais ainda, a classe de resíduo $\overline{3}$ não possui inverso multiplicativo, ou seja, $\overline{3}$ não é invertível. Este fato é consequência do máximo divisor comum de 3 e 9.

Definição 3.3.8 *O máximo divisor comum de dois inteiros a e b, denotado por $mdc(a, b)$, é o maior inteiro positivo que divide a e b.*

Teorema 3.3.7 *Se d é máximo divisor comum de a e b, então existem inteiros x_0 e y_0 tais que $d = ax_0 + by_0$.*

Demonstração Seja S o conjunto assim definido: $S = \{ax + by; x, y \in \mathbb{Z}\}$.
Tomemos $c = ax_0 + by_0$, com x_0 e y_0 inteiros e c o menor elemento de S. Provaremos que $d = c$.
Mostremos inicialmente que $c \mid a$ e $c \mid b$. Devido serem análogas as demonstrações iremos nos limitar a provar que $c \mid a$.

Suponhamos que $c \nmid a$. Pelo Algoritmo da divisão de Euclides, existem q e r tais que

$$a = qc + r \qquad com \qquad 0 \leq r < c.$$

Assim, temos

$$\begin{aligned} r &= a - qc \\ &= a - q(ax_0 + by_0) \\ &= a(1 - qx_0) + b(-qy_0), \end{aligned}$$

consequentemente $r \in S$. Logo, temos uma contadição, pois $0 \leq r < c$ e c é o menor elemento de S. Portanto, $c \mid a$ e $c \mid b$.

Como por hipótese $d \mid a$ e $d \mid b$, existem m e n tais que

$$a = md \qquad e \qquad b = nd,$$

Daí, segue que

$$\begin{aligned} c &= ax_0 + by_0 \\ &= x_0(md) + y_0(nd) \\ &= d(x_0m + y_0n). \end{aligned}$$

Logo, $d \mid c$ implicando em $d \leq c$. Como c é o menor elemneto de S, temos necessariamente $d = c$. Portanto, $d = ax_0 + by_o$ ■

Definição 3.3.9 *Dois inteiros a e b são primos entre si, quando $mdc(a, b) = 1$.*

Proposição 3.3.12 *Dois números a e b são primos entre si, se, e somente se, existem números inteiros m e n tais que $ma + nb = 1$.*

Demonstração ($\Rightarrow$) Se a e b são primos entre si, temos $mdc(a, b) = 1$. Daí, seque pelo Teorema 3.3.7 que existem m e n números inteiros tais que

$$ma + nb = 1.$$

($\Leftarrow$) Se existem números inteiros m e n tais que ma+nb=1. Se $d = mdc(a, b)$, segue que $d \mid ma + nb$ implicando em $d \mid 1$. Portanto, $d = 1$. ■

Proposição 3.3.13 *Um elemento $\overline{a} \in \mathbb{Z}_m$ é invertível se, e somente se, $mdc(a, m) = 1$.*

Demonstração ($\Rightarrow$) Se $\overline{a}$ é invertível, então pela Definição 3.3.7, existe $\overline{b} \in \mathbb{Z}_m$ tal que

$$\overline{1} = \overline{a} \cdot \overline{b} = \overline{ab}.$$

Assim, como $\overline{ab} = \overline{1}$ implica que $ab \equiv 1 \; mod \; m$. Segue da Definição 3.1.4 que

$$m \mid ab - 1.$$

Logo, existe $t \in \mathbb{Z}$ tal que $ab + tm = 1$. Portanto, $mdc(a, m) = 1$.

($\Leftarrow$) Se $mdc(a, m) = 1$, então pelo Teorema 3.3.7, existem números inteiros b e q tais que

$$ab + qm = 1.$$

Consequentemente, temos

$$\overline{1} = \overline{ab + qm} = \overline{ab} + \overline{qm} = \overline{a} \cdot \overline{b} + \overline{0} = \overline{a} \cdot \overline{b}.$$

Portanto, $\overline{a}$ é invertível. ■

Proposição 3.3.14 *Seja m um número não primo com $m = pq$ com $p > 1$ e $q > 1$. Se $\mathbb{Z}_m$ é o anel de inteiros módulo m, então:*

(i) *existem duas classes de resíduo, $\overline{r}$ e $\overline{s}$, não iguais a $\overline{0}$ tais que $\overline{r} \cdot \overline{s} = \overline{0}$;*

(ii) *nenhuma destas classes de resíduos, $\overline{r}$ e $\overline{s}$, têm inversos multiplicativos.*

Demonstração (i) Se $m = pq$, então $1 < p < m$ e $1 < q < m$. Sejam $\overline{r}, \overline{s} \in \mathbb{Z}_m$, tais que

$$r = p \qquad e \qquad s = q.$$

Como consequência da escolha de r e s, obtemos

$$rs = pq = m \Rightarrow \overline{rs} = \overline{m} \Rightarrow \overline{r} \cdot \overline{s} = \overline{0}.$$

Portanto, existem de fato $\overline{r}$ e $\overline{s}$, não iguais a $\overline{0}$ tais que $\overline{r} \cdot \overline{s} = \overline{0}$.

(ii) Suponhamos que $\overline{r}$ tenha inverso multiplicativo e seja $\overline{r'}$. Como por (i) $\overline{r} \cdot \overline{s} = \overline{0}$, temos

$$\overline{0} = \overline{r'} \cdot \overline{0} = \overline{r'} \cdot (\overline{r} \cdot \overline{s}) = (\overline{r'} \cdot \overline{r}) \cdot \overline{s} = \overline{1} \cdot \overline{s} = \overline{s}.$$

Logo, temos uma contradição uma vez que por (i) $\overline{s} \neq \overline{0}$. Portanto, $\overline{r}$ e $\overline{s}$ não possuem inversos multiplicativos. ■

Passemos ao estudo de $\mathbb{Z}_p$ com $p > 1$ primo. Recordamos que

$$\mathbb{Z}_p = \bigcup_{i=1}^{p-1} \overline{r},$$

com $0 \leq r < p$. Portanto, $mdc(r, p) = 1$, para todo $\overline{r} \neq \overline{0}$. Pela Proposição 3.3.13 acima, $\overline{r}$ tem um inverso multiplicativo. Mais ainda, se $\overline{r}$ e $\overline{s}$ não são a classe de resíduo zero, então $\overline{rs} \neq \overline{0}$. com efeito, suponha por absurdo que $\overline{rs} = \overline{0}$, por multiplicação em ambos os membros da igualdade pela inverso de $\overline{r}$, obtemos $\overline{s} = \overline{0}$, uma contradição.

3.4 Pequeno Teorema de Fermat

Seja $1 \leq p$ e $1 \leq i \leq p$ dois inteiros. Denotaremos por $\binom{p}{i}$ a combinação de p elementos i a i. Como sabemos

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}.$$

Lema 3.4.4 *Seja p uma número primo. Os números $\binom{p}{i}$, onde $0 < i < p$, são todos divisíveis por p.*

Demonstração Para $i = 1$ o resultado é válido, pois

$$\binom{p}{1} = \frac{p!}{p(p-1)!} = \frac{p(p-1)!}{p(p-1)!} = 1.$$

Podemos, então, supor $1 < i < p$. Neste caso, $i! \mid p(p-1)\cdots(p-i+1)$. Como $(i!, p) = 1$, tem-se que
$i! \mid (p-1)\cdots(p\cdots(p-i+1)$, e logo o resultado segue, pois

$$\binom{p}{i} = p\frac{(p-1)\cdots(p-i+1)}{(i!)}.$$

■

Teorema 3.4.8 (Pequeno Teorema de Fermat) *Se p é um número primo e $a \in \mathbb{N}$, então $a^p \equiv a \; mod \; p$.*

Demonstração Vamos provar usando Indução Matemática sobre a. Para $a = 1$ a afirmação é verdade. De fato,

$$1^p - 1 = 0 \quad \text{e} \quad p \mid 0.$$

Suponhamos que $a^p \equiv a \; mod \; p$ seja verdade para $a \in \mathbb{N}$. Vamos provar para $a + 1$.
Pelo binômio de Newton, temos

$$(a+1)^p - (a+1) = a^p - a + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}$$

Pelo Lema 3.4.4 e pela hipótese de indução, temos

$$p \mid a^p - a + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}$$

$$p \mid (a+1)^p - (a+1) \Rightarrow (a+1)^p \equiv a + 1 \; mod \; m.$$

Portanto $a^p \equiv a \; mod \; p$ para todo $a \in \mathbb{N}$. ■

Corolário 3.4.1 *Se p é primo, a é um número natural e $p \nmid a$ então $a^{p-1} \equiv 1 \; mod \; p$.*

Demonstração Pelo Pequeno Teorema de Fermat temos $p \mid a^p - a = a(a^{p-1} - 1)$ o que implica $p \mid a(a^{p-1} - 1)$ e como $(a, p) = 1$, segue-se que $p \mid a^{p-1} - 1$. Portanto

$$a^{p-1} \equiv 1 \; mod \; p.$$

■

4 A PROVA DOS NOVES FORA

Neste capítulo mostraremos uma breve contextualização histórica da prova dos noves, bem como a utilização do algoritmo nas operações fundamentais de adição, subtração, multiplicação e divisão e um critério para os onzes fora e setes fora.

4.1 Contexto Histórico

É bem verdade que a prova dos noves fez parte dos ensinos da escola antiga integrando os conteúdos dos livros didáticos. Historiadores como Bezerra afirmava ser uma prova muito utilizada antigamente para se verificar a validade dos cálculos em operações básicas.

> "Lembro que na época que iniciei a universidade e comecei a ministrar aulas, ensinávamos os alunos a decorar a tabuada e assim, na resolução de operações com números naturais ensinávamos além da prova real, também a "prova dos noves fora", que se encontra presente ainda nos livretos de tabuada, os quais são vendidos em papelarias do Estado, sendo que esta prova ainda é aplicada por alguns comerciantes locais (BEZERRA, 2013, p.9)."

Verdade que com o passar do tempo as escolas deixaram de utilizar a prova dos noves. Hoje raramente os discentes conhecem tal método. Isso se deve ao fato da escola atual não ver ou não entender a importância dos tópicos teóricos que tal processo traz consigo. A discussão que mais permeia é sobre a interpretação que se dá a prova dos noves que pode ser entendida como prática social, regra ou método. Como prática social, vê-se nitidamente o caráter cultural que ao longo do tempo foi sendo conferido entre comunidade e escola no que tange a verificação da exatidão ou não de um cálculo. Para Miguel, 2010 a prova se caracteriza não como um conteúdo autônomo e sim como uma prática social criada pela escola e para a escola.

> "[...] melhor seria conceber a prova dos noves como uma prática sociocultural de verificação da correção de um cálculo escrito, e não como um conteúdo escolar autônomo e interno que, tal como se postula na perspectiva de Chervel (1990), teria sido criado "na escola, pela escola e para a escola", ou então, como um suposto saber a ensinar que, tal como se postula na perspectiva de Chevallard (1991), teria sido transposto didaticamente da esfera sábia para o contexto escolar (MIGUEL,2010. p. 5)."

Nesta perspectiva incorre o fato de se ver a prova dos noves desvinculada de um conteúdo científico. Assim seria a escola a responsável pela produção dos seus saberes de forma que tal aprendizagem ficaria restrita ao ambiente escolar. Vista como regra, tem-se um conjunto de passos para verificação do correto desenvolvimento ou não de uma operação de adição, subtração, multiplicação e divisão. O pensamento em questão ressalta apenas a análise de acertos das operações e não menciona a observância de possíveis erros nos cálculos.

Vislumbrando sobre a ótica de método, tem-se uma apreciação, não sobre verificação de acertos das operações, e sim sobre a percepção de erros cometidos. Parece ser essa análise mais salutar, uma vez que veremos adiante ser a prova dos noves passível de falha. Assim, caracterizava-se por um método para identificar erros em operações com números naturais, além de se particularizar como aplicação das propriedades de congruência. Dessa forma, podemos perceber que apesar de não ser mais um recurso utilizado pela escola, a prova dos noves caracteriza-se por um método ainda muito utilizado por comerciantes para verificar possíveis erros cometidos nas operações básicas. Seja qual for a forma de entendermos vale o desprendimento na busca de sabermos quando e quais os indícios que relatam o seu surgimento que parece remotar à séculos.

Escritores árabes usavam a prova dos noves em seus tratados, pode-se citar o matemático al-Khowârizmi que viveu no século IX. Era comum o uso de cálculos modelados nos algoritmos hindus na aritmética árabe. Segundo Eves (2004), em seu livro *Introdução à História da Matemática*, a prova dos noves era um dos processos presentes na aritmética de al-Khowârizmi . No entanto, para Cajori em *Uma História da Matemática*, o teólogo Hipólito, século III, teria sido mencionado por ter dado método da prova de um cálculo denominado nove e setes fora. Dessa forma não se pode atribui diretamente aos hindus o processo da prova dos noves, uma vez que o método já era conhecido por Hipólito. Por outro lado nos cabe relatar que no *Tratado da Pratica d'Arismetyca Ordenada por Gaspar Nycolas* e impresso em 1519, em Lisboa, já se fazia menção a prova dos noves através de um exemplo numérico no qual explicava a forma de procedimento do método, sendo a primeira referência escrita em língua portuguesa.

4.2 O Noves Fora de um Número

O noves fora de um número natural n é subtrair o maior múltiplo de 9 menor que n. Existe um algoritmo eficiente para realizar tal subtração e determinar qual o resto da operação.

Uma boa ilustração do processo é o noves fora de 68,

$$68 = 9 \cdot 7 + 5 = 63 + 5,$$

como 63 é o maior múltiplo de 9 contido em 68 temos que o noves fora de 68 é 5 pois $68-63=5$. No entanto uma maneira prática de se obter o noves fora de um dado número natural consiste em somar os algarismos deste número até obter-se outro valor. A partir do novo valor, soma-se novamente os algarismos e assim consequentemente até restar um número de um único algarismo. Dessa forma para extrairmos o noves fora do número 683 aplicando o algoritmo prático procedemos da seguinte maneira:

$$\begin{aligned} 683 &\Rightarrow 6+8+3=17; \\ 17 &\Rightarrow 1+7=8. \end{aligned}$$

Logo, o noves fora de 683 é igual a 8. Justifiquemos tais procedimentos.

Proposição 4.2.15 *Seja $k=x_nx_{n-1}\cdots x_1x_0$ a representação decimal do natural k. O resto da divisão de k por 9 é o mesmo resto obtido pela divisão de $k'=x_n+x_{n-1}+\cdots+x_2+x_1+x_0$ por 9.*

Demonstração Mostremos inicialmente que $9 \mid 10^n-1$.

Com efeito, como provado no item (i) da Proposição 2.2.3, p.13, sabemos que $a-b \mid a^n-b^n$. Logo $10-1 \mid 10^n-1$, ou seja, $9 \mid 10^n-1$.

Passemos à demonstração da proposição. Sejam

$$k=10^nx_n+10^{n-1}x_{n-1}+\cdots+10x_1+x_0 \qquad \text{e} \qquad k'=x_n+x_{n-1}+\cdots+x_1+x_0,$$

números naturais, em que x_i é algarismo do sistema de numeração decimal com $i \in \mathbb{N}$, $0 \le i \le n$. Pelo algoritmo da divisão, podemos determinar números naturais q, q', r e r', com $0 \le r, r' < 9$, tais que

$$k=9q+r \qquad \text{e} \qquad k'=9q'+r'.$$

Agora,

$$\begin{aligned} k &= 10^nx_n+10^{n-1}x_{n-1}+\cdots+10x_1+x_0 \\ &= (10^n-1+1)x_n+(10^{n-1}-1+1)x_{n-1}+\cdots+(10-1+1)x_1+x_0] \\ &= [(10^n-1)x_n+(10^{n-1}-1)x_{n-1}+\cdots+(10-1)x_1]+(x_n+x_{n-1}+\cdots+x_1+x_0). \end{aligned}$$

Se $y=[(10^n-1)x_n+(10^{n-1}-1)x_{n-1}+\cdots+(10-1)x_1]$, pelo visto inicialmente temos $9 \mid y$, pois y é uma soma de múltiplos de 9. Escrevendo $y=9y''$ temos

$$\begin{aligned} k &= 9y'+(x_n+x_{n-1}+\cdot+x_1+x_0) \\ &= y+k'. \end{aligned}$$

Substituindo k, y e k' obtemos:

$$\begin{aligned} 9q + r &= 9q'' + 9q' + r' \\ 9q + r &= 9(q' + q'') + r'. \end{aligned}$$

Como $0 \leq r < 9$ e $0 \leq r' < 9$, tem-se que $r = r'$. Portanto k e k' deixam o mesmo resto quando divididos por 9. ■

O noves fora é uma aplicação sucessiva do processo acima apoiado no seguinte corolário, cuja demonstração é imediata.

Corolário 4.2.2 *Seja $k = x_n x_{n-1} \cdots x_1 x_0$ a representação decimal do natural k. O natural k é divisível por 9 se, e somente se, $k' = x_n + x_{n-1} + \cdots + x_1 + x_0$ é divisível por 9.*

O corolário também nos dá informações sobre congruência módulo 9, pois como mostrado na proposição $9 \mid k - k'$, ou seja,

$$x_n x_{n-1} \cdots x_1 x_0 \equiv x_n + x_{n-1} + \cdots + x_1 + x_0.$$

Além disto nos dá informações sobre o resto da divisão de k por 9, pois

$$\overline{x_n x_{n-1} \cdots x_1 x_0} = \overline{x_n + x_{n-1} + \cdots + x_1 + x_0},$$

em $\mathbb{Z}_9$.

Exemplo 4.2.8 Calculemos o noves fora de 3 475 aplicando sucessivamente a Proposição 4.2.15, acima. Isto nos dá um algoritmo simples para calcular qual a classe de resíduo em $\mathbb{Z}_9$ o número pertence,

$$\begin{aligned} \overline{3\,475} &= \overline{19} \\ &= \overline{10} \\ &= \overline{1}. \end{aligned}$$

A resposta obtida, congruência com 1, significa que o resto da divisão de 3 475 por 9 tem resto 1, ou seja $3\,475 \in \overline{1}$, portante ele se escreve como $3\,475 = 9m + 1$. ◇

4.3 A Prova dos Noves para Adição

Proposição 4.3.16 *O noves fora de uma soma é igual a soma dos noves fora de cada parcela.*

Demonstração Sejam x, y e z números inteiros tais que $x + y = z$, segue imediato da Definição 3.2.5, p. 29 que

$$\overline{z} = \overline{x + y} = \overline{x} + \overline{y}.$$

■

Exemplo 4.3.9 Vamos determinar o noves fora da soma $578 + 49 = 627$.

$$\overline{578 + 49} = \overline{627} = \overline{6 + 2 + 7} = \overline{6 + 9} = \overline{6} + \overline{9} = \overline{6} + \overline{0} = \overline{6}.$$

Portanto, o noves fora de $578 + 49$ é igual a 6.

4.4 A Prova dos Noves para Subtração

Proposição 4.4.17 *O noves fora da soma dos noves fora do subtraendo e do resultado é igual noves fora do minuendo.*

Demonstração Sejam x, y e z números inteiros tais que $x - y = z$. Pela Definição 3.2.5, p. 29 e como foi provado nos itens (i),(ii) e (iii) da Proposição 3.2.8, p. 30, temos

$$\begin{aligned}
\overline{x - y} &= \overline{z};\\
\overline{x} + \overline{-y} &= \overline{z};\\
\overline{x} + \overline{-y} + \overline{y} &= \overline{z} + \overline{y};\\
\overline{x} + \overline{y} + \overline{-y} &= \overline{z} + \overline{y};\\
\overline{x} + \overline{0} &= \overline{z} + \overline{y};\\
\overline{x} &= \overline{z} + \overline{y}.
\end{aligned}$$

■

Exemplo 4.4.10 Vamos determinar o noves fora da subtração $872 - 321 = 551$

$$\overline{872 - 321} = \overline{551} = \overline{5 + 5 + 1} = \overline{11} = \overline{1 + 1} = \overline{2}.$$

Portanto, o noves fora de $872 - 321$, é igual 2.

4.5 A Prova dos Noves para a Multiplicação

Proposição 4.5.18 *O noves fora do produto dos noves fora dos fatores é igual ao noves fora do resultado.*

Demonstração Sejam x, y e z números inteiros tais que $x \cdot y = z$. Pela Definição 3.2.6, p. 31, temos

$$\overline{z} = \overline{x \cdot y} = \overline{x} \cdot \overline{y}$$

■

Exemplo 4.5.11 Vamos determinar o noves fora do produto $672 \cdot 21 = 14112$.

$$\overline{672 \cdot 21} = \overline{14112} = \overline{1 + 4 + 1 + 1 + 2} = \overline{9} = \overline{0}.$$

Portanto, o noves fora de $672 \cdot 21$ é igual a 0.

4.6 A Prova dos Noves para a Divisão

Proposição 4.6.19 *O noves fora, do produto do noves fora do quociente e do divisor somado com o noves fora do resto, é igual ao noves fora do dividendo.*

Demonstração Sejam x y, q e r números inteiros tais que $y = qx + r$, com $0 \leq r < x$. Pelas Definições 3.2.5 e 3.2.6, pp. 29 e 31, temos

$$\overline{y} = \overline{qx + r} = \overline{qx} + \overline{r} = \overline{q} \cdot \overline{x} + \overline{r}.$$

■

Exemplo 4.6.12 Vamos determinar o noves fora da divisão $832 : 21$.
Como $832 = 39 \cdot 21 + 13$, temos

$$\begin{aligned}
\overline{832} &= \overline{39 \cdot 21 + 13} \\
&= \overline{39 \cdot 21} + \overline{13} \\
&= \overline{39} \cdot \overline{21} + \overline{13} \\
&= \overline{39} \cdot \overline{21} + \overline{1 + 3} \\
&= \overline{39} \cdot \overline{21} + \overline{4}.
\end{aligned}$$

Portanto, o noves fora de $832 : 21$ é igual a 4.

4.7 Um Critério para Onzes Fora e Setes Fora

Inicialmente iremos generalizar a Proposição 4.2.15, p. 39 para uma base b qualquer.

Sejam

$$k = b^n x_n + b^{n-1} x_{n-1} + \cdots + b x_1 + x_0 \qquad e \qquad k' = x_n + x_{n-1} + \cdots + x_1 + x_0,$$

números naturais, em que x_i é algarismo do sistema de numeração decimal com $i \in \mathbb{N}$, $0 \leq i \leq n$. Pelo algoritmo da divisão, podemos determinar números naturais q, q', r e r', com $0 \leq r, r' < (b-1)$, tais que

$$k = (b-1)q + r \qquad e \qquad k' = (b-1)q' + r'.$$

Agora,

$$\begin{aligned} k &= b^n x_n + b^{n-1} x_{n-1} + \cdots + b x_1 + x_0. \\ &= [(b^n - 1 + 1)x_n + (b^{n-1} - 1 + 1)x_{n-1} + \cdots + (b - 1 + 1)x_1 + x_0]. \\ &= [(b^n - 1)x_n + (b^{n-1} - 1)x_{n-1} + \cdots + (b-1)x_1] + (x_n + \cdots + x_1 + x_0). \end{aligned}$$

Se $y = [(b^n - 1)x_n + (b^{n-1} - 1)x_{n-1} + \cdots + (b-1)x_1]$, pelo visto inicialmente temos $(b-1) \mid y$, pois y é uma soma de múltiplos de $(b-1)$. Escrevendo $y = (b-1)y''$ temos

$$\begin{aligned} k &= (b-1)y'' + (x_n + x_{n-1} + \cdots + x_1 + x_0). \\ &= y + k'. \end{aligned}$$

Substituindo k, y e k' obtemos:

$$\begin{aligned} (b-1)q + r &= (b-1)q'' + (b-1)q' + r'. \\ (b-1)q + r &= (b-1)(q' + q'') + r'. \end{aligned}$$

Como $0 \leq r < (b-1)$ e $0 \leq r' < (b-1)$, temos $r = r'$. Portanto k e k' deixam o mesmo resto quando divididos por $(b-1)$.

Recordermos que $[x_n, \ldots, x_0]_b = b^n x_n + b^{n-1} x_{n-1} + \cdots + b x_1 + x_0$,

Analisando o que foi exposto acima, concluímos que se $k = [x_n, \ldots, x_0]_b$, então

$$k \equiv x_o + x_1 + \cdots + x_n \; mod \; b - 1.$$

Portanto, temos em $\mathbb{Z}_{(b-1)}$ que $\overline{k} = \overline{x_o + x_1 + \cdots + x_n}$. Assim o $(b-1)$'s fora de k é igual ao $(b-1)$'s fora do número formado pela soma dos dígitos de sua representação na base b.

Para construímos os critérios dos onzes fora e dos setes fora basta que b assuma, respectivamente, os valores 12 e 8. Dessa forma, temos

(1) Se $k = [a_n, \ldots, a_1, a_0]_{12}$, então $\overline{k} = \overline{a_0 + a_1 \cdots +, a_n}$.

(2) Se $k = [b_n, \ldots, b_1, b_0]_8$, então $\overline{k} = \overline{b_0 + b_1 \cdots +, b_n}$.

Exemplo 4.7.13 Determinar o onzes fora de 1 257.

Inicialmente iremos representar 1 257 na base 12 :

$$\begin{aligned} 1\,257 &= 104 \cdot 12 + 9; \\ 104 &= 8 \cdot 12 + 8; \\ 8 &= 0 \cdot 12 + 8. \end{aligned}$$

Logo, $1\,257 = [889]_{12}$. Assim, temos

$$\overline{1\,257} = \overline{8 + 8 + 9} = \overline{25} = \overline{22 + 3} = \overline{3}.$$

Portanto, o onzes fora de 1 257 é igual a 3.

Exemplo 4.7.14 Determinar o setes foras de 3 726.

Vamos representar 3 726 na base 8 :

$$\begin{aligned} 3\,726 &= 465 \cdot 8 + 6; \\ 465 &= 58 \cdot 8 + 1; \\ 58 &= 7 \cdot 8 + 2; \\ 7 &= 0 \cdot 8 + 7. \end{aligned}$$

Logo, $3\,726 = [7216]_8$. Daí, temos

$$\overline{3\,726} = \overline{7 + 2 + 1 + 6} = \overline{14 + 2} = \overline{2}$$

Portanto, o setes fora de 3 726 é igual a 2.

Exemplo 4.7.15 Determinar o dozes foras de 376.

Vamos representar 376 na base 13:

$$\begin{aligned} 376 &= 28 \cdot 13 + 12; \\ 28 &= 2 \cdot 13 + 2; \\ 2 &= 0 \cdot 13 + 2. \end{aligned}$$

Logo $376 = [22\lambda]_{13}$, em que $\lambda = 12$. Daí, temos

$$\overline{376} = \overline{2 + 2 + \lambda} = \overline{2 + 2 + 12} = \overline{4 + 12} = \overline{4}$$

Portanto, o dozes fora de 376 é igual a 4.

5 CONTROVÉRSIAS E APLICAÇÕES

5.1 A Falha da Prova dos Noves

Um dos questionamentos que podemos fazer sobre a prova dos noves é se existe a possibilidade de aplicação da regra com outro número além do nove. Quanto a esta questão se pode afirmar que não há nenhuma restrição teórica. Na verdade poderíamos está realizando a prova dos setes fora, dos onzes fora ou de qualquer outro número. No entanto o motivo pelo qual utilizamos a prova dos noves fora se dá por duas razões. A primeira de ordem prática, pois é muito mais simples encontramos o resto de uma divisão por nove que o resto de uma divisão, por exemplo, por onze. A segunda pelo fato do nosso sitema de numeração ser decimal. Caso nosso sistema tivesse base 13 estaríamos certamente falando em prova dos dozes fora e não dos noves fora.

Um outro contraponto é sobre a infabilidade da prova dos noves. É muito comum ouvirmos relatos de que estando certa a prova a operação também estará. Essa convicção é apreciada ainda hoje pelos que fizeram parte dos ensinamentos da escola antiga, refiro-me aos nossos pais, tios e avós. Geralmente a prova era apresentada, pelos mais velhos, apenas para a operação de adição e tida como um método irrefutável para verificação da correta realização da conta. Não se admitia a possibilidade de falha na prova. Mostraremos que esse pensamento de infabilidade é errôneo. Quanto a essa reflexão se pode afirmar que quando a prova dos noves está correta ela nada garante sobre a exata realização da operação podendo a mesma ter sido realizada ou não de forma certa. Quando há inversão na ordem dos algarismos do resultado a prova não detecta o erro cometido na conta já que a ordem das parcelas não altera a soma e assim ambos os valores obtidos deixarão o mesmo resto na divisão por nove.

Proposição 5.1.20 *Se k e k' são dois números inteiros, com k' obtido a partir da permutação dos algarismos de k então ambos deixam o mesmo resto quando divididos por* 9.

Demonstração

Seja $k = x_n10^n + x_{n-1}10^{n-1} + \cdots + x_i10^i + + x_j10^j + \cdots + x_2 10^2 + x_1 10 + x_0$, com i e $j = 1,2,\ldots,n$, i e j números naturais.

Escrevendo k da seguinte forma:

$$k = x_n(10^n - 1 + 1) + x_{n-1}(10^{n-1} - 1 + 1) + \cdots + x_i(10^i - 1 + 1) + \cdots + x_j(10^j - 1 + 1) + \cdots + x_2(10^2 - 1 + 1) + x_1(10 - 1 + 1) + x_0.$$

$$k = x_n(10^n - 1) + x_{n-1}(10^{n-1} - 1) + \cdots + x_i(10^i - 1) + \cdots + x_j(10^j - 1) + \cdots + x_2(10^2 - 1) + x_1(10 - 1) + (x_n + x_{n-1} + \cdots + x_i + \cdots + x_j + \cdots + x_2 + x_1 + x_0).$$

Utilizando o fato de $(10^n - 1)$ ser um múltiplo de 9 temos

$$k = (9p_n)x_n + (9p_{n-1})x_{n-1} + \cdots + 9p_ix_i + \cdots + 9p_jx_j + \cdots + 99x_2 + 9x_1 + (x_n + x_{n-1} + \cdots + x_i + \cdots + x_j + \cdots + x_2 + x_1 + x_0).$$

Seja k' o número obtido pela inversão de um x_i por um x_j.

$$k' = (9p_n)x_n + (9p_{n-1})x_{n-1} + \cdots + 9p_ix_j + \cdots + 9p_jx_i + \cdots + 99x_2 + 9x_1 + (x_n + x_{n-1} + \cdots + x_i + \cdots + x_j + \cdots + x_2 + x_1 + x_0).$$

Tomando $r = (x_n + x_{n-1} + \cdots + x_i + \cdots + x_j + \cdots + x_2 + x_1 + x_0)$ podemos escrever k e k' da seguinte forma,

$$k = 9p + r \text{ e } k' = 9p' + r.$$

Portanto k e k' deixam o mesmo resto na divisão por 9. ■

Observação 5.1.2 *Da demonstração podemos concluir que $k - k'$ é sempre um múltiplo de nove.*

Como exemplo tomemos o produto $235 \cdot 123 = 28\,905$, caso o resultado obtido fosse 29 805 a prova dos noves não acusaria a falha cometida pois $29\,805 - 28\,905 = 900$ que é um múltiplo inteiro de 9.

5.2 Aplicações

Problema 1 Efetue a adição e multiplicação dos números 576 e 984 e tire a prova dos noves para as duas operações.

Resolução
(i) Adição

Como $576 + 984 = 1\,560$:

(1) $\overline{576} + \overline{984} = \overline{5 + 7 + 6} + \overline{9 + 8 + 4} = \overline{18} + \overline{21} = \overline{0} + \overline{3} = \overline{3}$;

(2) $\overline{1\,560} = \overline{1 + 5 + 6 + 0} = \overline{12} = \overline{3}$.

Portanto, $\overline{576} + \overline{984} = \overline{1\,560} = \overline{3}$.
ii) Multiplicação

Como $576 \cdot 984 = 566\,784$, temos:

(1) $\overline{576} \cdot \overline{984} = \overline{5 + 7 + 6} \cdot \overline{9 + 8 + 4} = \overline{18} \cdot \overline{21} = \overline{0} \cdot \overline{3} = \overline{0}$;

(2) $\overline{566\,784} = \overline{5+6+6+7+8+4} = \overline{36} = \overline{9} = \overline{0}$.

Portanto, $\overline{576} \cdot \overline{984} = \overline{566\,784} = \overline{0}$. ◇

Problema 2 Chamamos de excesso de um número o resto obtido ao se dividir esse número por 9.
Prove as afirmações a seguir:

(1) O excesso de uma soma é igual ao excesso da soma dos excessos das parcelas.

(2) O excesso do produto de dois números é igual ao excesso do produto dos excessos dos dois números.

Resolução A definição dada para o termo *excesso* de um número, equivale a classe de resíduo de $\mathbb{Z}_9$ a qual esse número pertence. Usaremos as definições para soma e multiplicação entre elementos de $\mathbb{Z}_9$ para resolução dos itens (1) e (2).
Sejam x, y e z números inteiros, temos

$$\begin{cases} (1)\ \ x + y = z \Rightarrow \overline{z} = \overline{x+y} = \overline{x} + \overline{y}. \\ (2)\ \ x \cdot y = z \Rightarrow \overline{z} = \overline{x \cdot y} = \overline{x} \cdot \overline{y}. \end{cases}$$

◇

Problema 3 Mostre que permutando-se de qualquer maneira a ordem dos algarismos de um número natural, então a diferença entre o número original e o que se obteve é divisível por 9.

Resolução Seja P um número natural e Q o número obtido por qualquer permutação dos algarismos de P. Como P e Q possuem mesmos algarismos pelo que foi provado na Proposição 5.1.20, p. 46 ambos deixam o mesmo resto na divisão por 9.
Dessa forma, podemos escrever

$$\begin{aligned} P &= 9m + r \ e \ Q = 9n + r; \\ P - Q &= 9m + r - 9n - r; \\ P - Q &= 9(m-n) \Rightarrow 9 \mid P - Q. \end{aligned}$$

Portanto, $P - Q$ é divisível por 9. ◇

Problema 4 Explique o seguinte truque: Pede-se a alguém que pense num número; forme um novo número invertendo a ordem dos algarismos; subtrai o menor do maior; multiplique a diferença por um número qualquer; tire fora um digíto qualquer do produto; e anuncie o que restou. Encontra-se-á o dígito que foi tirado fora fazendo-se a diferença entre 9 e o excesso do resultado anunciado.

Resolução Como a diferença entre dois numeros naturais, em que um é obtido a partir da inversão dos algarismos do outro, é sempre um múltiplo de nove o resultado do produto tem excesso zero. Pelo fato do excesso da soma dos algarismos de um número ser igual ao excesso do próprio número, tem-se que o excesso da soma dos algarismos do número obtido no produto deve ser zero. Assim o excesso do número anunciado mais o dígito que foi retirado é igual a nove. Portanto o digíto retirado é a diferença entre nove e o excesso do número anunciado. ◇

Problema 5 Teste a adição $104 + 454 + 1\,096 + 2\,195 + 3\,566 + 4\,090 = 11\,505$ tirando os onzes fora.

Temos

$$\begin{aligned}
\overline{104 + 454 + 1\,096 + 2\,195 + 3\,566 + 4\,090} &= \overline{104} + \overline{454} + \overline{1\,096} + \overline{2\,195} + \overline{3\,566} + \overline{4\,090} \\
&= \overline{99 + 5} + \overline{451 + 3} + \overline{1\,089 + 7} + \overline{2\,189 + 6} + \overline{3\,564 + 2} + \\
&\quad + \overline{4\,081 + 9} \\
&= \overline{5} + \overline{3} + \overline{7} + \overline{6} + \overline{2} + \overline{9} \\
&= \overline{5 + 3 + 7 + 6 + 2 + 9} = \overline{22 + 10} = \overline{10}
\end{aligned}$$

Da mesma forma,

$$\overline{11\,505} = \overline{11\,495 + 10} = \overline{10}.$$

Portanto, $\overline{104 + 454 + 1\,096 + 2\,195 + 3\,566 + 4\,090} = \overline{11\,505} = \overline{10}$.

Problema 6 Mostre que o noves fora de $10^n + 3 \cdot 4^{n+2} + 5$ é igual a zero para todo $n \in \mathbb{N}$.

Resolução Sabemos que o noves fora de um número narual k é igual a zero se, somente se, $9 \mid k$. Vamos mostrar que $9 \mid 10^n + 3 \cdot 4^{n+2} + 5$ para todo $n \in \mathbb{N}$. Faremos indução sobre n.
A afirmação é verdade para $n = 1$. De fato,

$$10^1 + 3 \cdot 4^{1+2} + 5 = 207.$$

Como $9 \mid 207$, logo o noves fora de 207 é igual a zero. Suponhamos que $9 \mid 10^n + 3 \cdot 4^{n+2} + 5$. para todo $n \in \mathbb{N}$. Escrevendo

$$\begin{aligned}
10^{n+1} + 3 \cdot 4^{(n+1)+2} + 5 &= 10^n \cdot 10 + 3 \cdot 4^{n+2} \cdot 4 + 5 \\
&= 4 \cdot \left(10^n + 3 \cdot 4^{n+2} + 5\right) + 6 \cdot 10^n - 3 \cdot 5 \\
&= 4 \cdot \left(10^n + 3 \cdot 4^{n+2} + 5\right) + 6 \cdot 10^n - 6 - 9 \\
&= 4 \cdot \left(10^n + 3 \cdot 4^{n+2} + 5\right) + 6 \cdot \left(10^n - 1\right) - 9.
\end{aligned}$$

Pelo fato de $9 \mid 9$, $9 \mid (10^n - 1)$ e por hipótese de indução $9 \mid 10^n + 3 \cdot 4^{n+2} + 5$, segue que

$$9 \mid 10^{n+1} + 3 \cdot 4^{(n+1)+2} + 5,$$

ou seja, o noves fora de $10^{n+1} + 3 \cdot 4^{(n+1)+2} + 5$ é igual a zero.
Portanto, o noves fora de $10^n + 3 \cdot 4^{n+2} + 5$ é igual a zero para todo $n \in \mathbb{N}$. ◇

Problema 7 Determine o setes fora de 37^{45}.

Resolução Usando o Teorema 3.4.8, p. 36 e a Proposição 3.2.11, p. 32, temos:

$$37^7 \equiv 37 \equiv 2 \; mod \; 7 \Rightarrow (37^7) \equiv 2^6 \equiv 1 \; mod \; 7;$$

$$37^{42} \cdot 37^3 \equiv 1 \cdot 37^3 \; mod \; 7 \Rightarrow 37^{45} \equiv 50\,653 \equiv \; mod \; 7.$$

Logo, segue em $\mathbb{Z}_7$ que

$$\overline{37^{45}} = \overline{50\,653} = \overline{50\,652 + 1} = \overline{1}.$$

Portanto, o setes fora de 37^{45} é igual a 1. ◇

Problema 8 Mostre que o noves fora de $7\,202^5$ possui inverso multiplicativo em $\mathbb{Z}_9$.

Resolução Pela Proposição 4.2.15, p. 39, temos $7\,202 \equiv 7 + 2 + 0 + 2 \equiv 2$. Segue pela Proposição 3.2.11, p. 32 que

$$7\,202^5 \equiv 2^5 \equiv 32 \equiv 5.$$

Daí, $\overline{7\,202^5} = \overline{5}$. Como $\overline{2} \in \mathbb{Z}_9$ e $\overline{5} \cdot \overline{2} = \overline{1}$, concluimos que $\overline{5}$ possui inverso multiplicativo. ◇

6 CONSIDERAÇÕES FINAIS

Entender a prova dos noves fora apenas como uma prática cultural ou método para verificar as operções básicas é minimizar a importância de conceitos aritméticos que a prova consigo traz. Critérios de divisibilidade, sistema de numeração e congruência são indispensáveis para uma fundamentação teórica da prova.

Apesar do método ser uma condição necessária e não suficiente para determinar se uma operação foi realizada corretamente, sua abordgem nos apresenta proposições matemáticas relevantes. O próprio entendimento do porquê pode ocorrer falha na prova dos noves requer uma boa análise matemática.

Por outro lado temos a convicção que tal prova remota a séculos e que no Brasil era abordado nos ensinos da escola antiga e cobrado nos exames de admissão nos anos de 50 e 60, mostrando-se dessa forma a importância dada ao noves fora. Atualmente já não mais faz parte dos tópicos ministrados em matemática pela a escola e sua discussão vem sendo relegada ao esquecimento. É possível que esse descaso tenha sido um alerta para a desvalorização do ensino de aritmética que hoje se percebe.

Assim o presente trabalho visa contribuir com uma análise mais sólida sobre o noves fora. Alertar para a significância teórica da prova e de suas possíveis generalizações, refutar o pensamento que a mesma é uma mera averiguação das operações fundamentais. Por fim, advertir para a necessidade de uma melhor atenção nos ensinos de aritmética nas escolas de educação básica.

REFERÊNCIAS

[1] HEFEZ, Abramo. **Elementos de Aritmética**. 2. ed. Rio de Janeiro: SBM, 2011.

[2] EVES, Howard. **Introdução à História da Matemática**. Tradução: Hygino H. Domingues. São Paulo: Editora da UNICAMP, 2004.

[3] SANTOS, José Plínio de Oliveira. **Introdução a Teoria dos Números**. 3. ed. Rio de Janeiro: IMPA, 2011.

[4] LIMA, Elon Lages. **Números e Funções Reais**. Coleção PROFMAT. 1. ed. Rio de Janeiro: SBM, 2013.

[5] RODRIGUES, Flávio Wagner. **A Prova dos Noves**. Revista do Professor de Matemática, n. 14. Rio de Janeiro: SBM, 2009.

[6] ALENCAR FILHO, Edgard. **Teoria Elementar dos Números**. 3. ed. São Paulo: Nobel, 1992.

[7] BOYER, Carl B. **História da Matemática**. Tradução: Elza F. Gomide. 2. ed. São Paulo: Edgard Blücher, 1996.

[8] MORAIS FILHO, Daniel Cordeiro de. **Manual de Redação Matemática**. Coleção do Professor de Matemática. 1. ed. Rio de Janeiro: SBM, 2014.

[9] CHEVALLARD, Y; BOSCH, M; GASCÓN, J. **Estudar Matemática: o elo pedido entre o ensino e a apreendizagem**. Porto Alegre: Artmed, 2001.

[10] CAJORI, F. **Uma História de Matemática**. Rio de Janeiro: Ciência Moderna, 2007.

[11] BEZERRA, S. **Como me tornei uma professora de matemática: mémorias resgatadas através da história da Educação Matemática**. ENCONTRO NACIONAL DE EDUCAÇÃO MATEMÁTCA (ENEM), 2013, Curitiba. **Anais ...**. Belo Horizonte: Universidade Federeal de Minas Gerais, Sociedade Brasileira de Educação Matemática (SBEM), 2013.

[12] MIGUEL, A; SOUZA, E. da S. **Um estudo sobre o processo de obsolescência de uma prática cultural: a prova dos nove**. SEMINÁRIO INTERNACIONAL DE PESQUISA EM EDUCAÇÃO MATEMÁTICA(SIPEM), 3, 2006, Belo Horizonte. **Anais ...** Belo Horizonte: Universidade Federeal de Minas Gerais, Sociedade Brasileira de Educação Matemática (SBEM), 2006.