# CONGRUÊNCIAS E CRIPTOGRAFIA: UMA APROXIMAÇÃO ENTRE TEORIA DOS NÚMEROS E ESCOLA BÁSICA

**Lucas Santos Silva** – lucas.santos7904l@hotmail.com
Universidade do Estado do Pará
Belém - Pará

**Raimundo Flavio de Moraes Neto** – r.moraesneto@aluno.uepa
Universidade do Estado do Pará
Belém - Pará

**Marcos Vinicius Macedo de Andrade** – marcos.vmd.andrade@aluno.uepa.br
Universidade do Estado do Pará
Belém - Pará

**Rubens Vilhena Fonseca** – rubens.vilhena@uepa.br
Universidade do Estado do Pará
Belém - Pará

***Resumo:***

*O presente artigo se enquadra no eixo temático da Matemática Aplicada e tem o objetivo de apresentar, em nível elementar, noções de congruência, um tópico da Teoria dos Números, considerada a "Rainha da Matemática", para os que atuam na Escola Básica. O artigo pretende mostrar que, mesmo em nível elementar, é possível fazer uma conexão entre os assuntos congruência e criptografia. Através desses tópicos, procura-se destacar o poder e a elegância dos argumentos baseados na Teoria dos Números. Além disso, com a criptografia, é possível descrever a utilidade da Teoria Elementar dos Números em fornecer exposição a ideias matemáticas e apresentar, aos que atuam na Escola Básica, a essência da atividade matemática.*

**Palavras-chave:** teoria dos números; congruências; criptografia; escola básica.

**Área e Nível de Ensino:** Matemática - Ensino Médio.

## 1 INTRODUÇÃO

É final de mais um dia de trabalho e você dirige para sua casa. Em seu carro, você pressiona um controle remoto que abre o portão da garagem e você entra. Você pressiona o controle remoto novamente e o portão da garagem se fecha.

Entretanto, sem que você saiba, alguém mal-intencionado está à espreita na sua rua com um *scanner* de rádio que capta o sinal do seu controle remoto. Da próxima vez que você não estiver em casa, esse mal-intencionado planeja usar o sinal salvo para abrir o portão da garagem e praticar furtos. No entanto, no dia em que faz isso e envia o sinal, o portão não abre.

Agora suponha que você quer fazer uma compra na *internet* usando um cartão de crédito. Você deve ter notado que o http:// típico, que precede um endereço da *web*, é substituído por https://. O "s" no final indica um *site* seguro. Isto significa que alguém, que pode estar tentando roubar informações de cartão de crédito, não pode interceptar as informações que você envia.

Embora um controle remoto para abrir portão de garagem e um *site* seguro possam parecer bastante diferentes, a matemática por trás de cada um deles é semelhante. Ambos são baseados em Aritmética modular ou congruências, um importante assunto em Teoria dos Números.

A teoria elementar dos números possui muitos assuntos que podem enriquecer sobremaneira o processo de ensino e aprendizagem de Matemática na escola básica. Escolhemos algumas aplicações elementares em criptografia pela sua atualidade e pelos excelentes desafios e inter-relações que podem ser feitas com assuntos ministrados na educação básica (Baile, 1964).

Neste contexto, o presente artigo tem o objetivo de apresentar, em nível elementar, noções de congruência, um tópico da Teoria dos Números, considerada a "Rainha da Matemática", para os que atuam na Escola Básica.

## 2 APORTE TEÓRICO

A intenção deste artigo é favorecer a precisão, clareza e relevância da proposta apresentada. Acreditamos que, sob essa perspectiva, podemos oferecer uma grande oportunidade de apresentar aos professores da educação básica aplicações da matemática que são empolgantes e desempenham um papel importante (Dante, 2002), embora às vezes oculto, em nossas atividades diárias, servindo, dessa maneira, como um modo de criar interesse pela participação na disciplina nessas novas formas metodológicas que o momento atual exige (Brasil, 2015).

A Teoria das Congruências e sua aplicação na criptografia das informações são usadas não apenas pelas pessoas no seu dia a dia e pelos governos para manter as comunicações em segredo, mas também por bancos e outras empresas para proteger informações confidenciais

(Burton, 2016). Com o número crescente de transações que ocorrem na internet, a criptografia é de importância cada vez maior.

Muitas pessoas têm a impressão equivocada de que a Aritmética (e a Matemática de forma geral) é um assunto estático, no qual tudo já se sabe há centenas de anos. Assuntos como congruências e criptografia atuam como uma janela para as questões abertas e a natureza evolutiva da Matemática e, em particular, para a Teoria dos Números, muitas vezes considerada apenas como um playground divertido para não matemáticos, com pouca relevância para o mundo real. Nossa intenção é, com nossos futuros professores, cooperar para que essa visão seja revertida (Mendonça, 1993).

Pela necessidade de incorporar diversas habilidades matemáticas (fatoração, exponenciação, números primos, aritmética modular etc.) e utilizá-las de forma concreta, os participantes podem ser estimulados ao pensamento algorítmico crítico e o senso de praticidade e, desse modo, envolver seus alunos e manter o interesse deles durante toda a aplicação dessa proposta.

## 3 PROCEDIMENTOS METODOLÓGICOS

Uma vez que o tema da divisibilidade e restos (resíduos) é relativamente complexo com provas algébricas, estaremos aqui nos aproximando desse assunto de forma gradual, tendo em vista uma aproximação do assunto na educação básica. Começaremos com um caso em particular: vamos explorar a divisibilidade por 3. Essa abordagem nos ajudará a pavimentar nosso caminho para uma teoria avançada da divisibilidade (Schroeder; Lester, 1989). As ideias e técnicas que discutiremos hoje ilustrarão plenamente o modelo geral; no entanto, nossas provas serão mais "leves" do que provas de divisibilidade "gerais". Além disso, os problemas de restos (ou resíduos) por três são interessantes por si só e têm seu lugar único na coleção de questões desafiadoras sobre a divisibilidade.

### 3.2 Uma Aritmética dos Resíduos

3.2.1 Resíduos (restos) quando dividimos por 3

Vamos começar a discussão principal com um lembrete sobre *paritismo*[1] *ou paridade* nos inteiros: uma técnica simples, mas poderosa na resolução de questões aritméticas, que é muito útil para uma grande variedade de questões.

[1] O paritismo é definido por um resíduo: um número é *par* quando, ao ser dividido por 2, deixa resíduo 0; é *ímpar* quando o resíduo é 1.

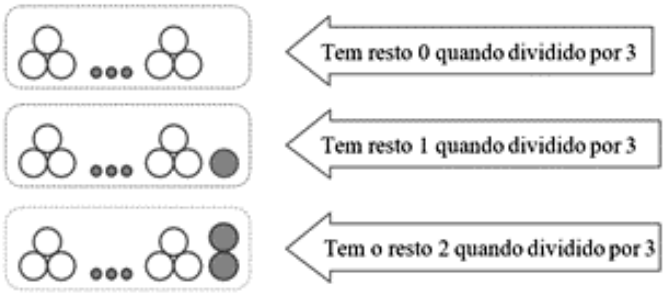
Na apostila “Encontros de Aritmética” (Cadar; Dutenhefner, 2015), temos o “Jogo das faces”, que mostra um jogo aritmético usando moedas onde se pode fazer atividades matemáticas mágicas, como aplicação dos resíduos de uma divisão por 2.

Se os resíduos, após uma divisão por 2, podem ser tão úteis na resolução de desafios aritméticos, os resíduos de divisões por outros números poderiam também ser tão úteis? A resposta é com toda certeza afirmativa. E foi uma resposta definitiva, dada a essa pergunta pelo matemático alemão Johann Carl Friedrich Gauss (1777-1855), que deu origem à Teoria das Congruências, e colocou a Aritmética na posição de destaque que hoje ocupa na Matemática.

Vamos começar explorando a divisibilidade por 3 e aprenderemos a usá-la na resolução de alguns desafios aritméticos. Começamos definindo todos os termos relacionados à divisão de números inteiros não negativos {0, 1, 2, 3,...} por 3. Assim: O número X tem resíduo 0 quando dividido por 3, se X = 3K. O número X tem o resíduo 1 quando dividido por 3, se X = 3K + 1. O número X tem o resíduo 2 quando dividido por 3, se X = 3K + 2.

Essa definição formal torna muito mais fácil provar questões sobre divisibilidade e restos. Para quem está iniciando, também é útil ter em mente um modelo visual da divisibilidade por 3 (Figura 1).

Figura 1 – Modelo visual da divisibilidade por 3




Fonte: Elaborado pelos autores (2022)

Também podemos considerar uma definição “informal” de um resíduo: “o menor número inteiro não negativo que, se subtraído, nos leva a um múltiplo de 3”. Vamos ilustrar essas definições:

- O número 36 tem resíduo 0 quando dividido por 3. De fato, 36 pode ser dividido em 12 grupos de 3 e pode ser escrito como $36=3\times12$. Assim, 36 não precisa ser subtraído de nenhum valor para ser múltiplo de 3.
- O número 19 tem resíduo 1 quando dividido por 3. De fato, 19 pode ser dividido em 6 grupos de 3 e deixar um resíduo igual a 1 e pode ser escrito como $19=3\times6+1$. Assim, o menor número inteiro não negativo, subtraído de 19, de modo a termos

um múltiplo de 3 seria o 1.

- O número 26 tem resíduo 2 quando dividido por 3. De fato, 26 pode ser dividido em 8 grupos de 3 e deixar um resíduo igual 2 e pode ser escrito como 26=3×8+2. Assim, o menor número inteiro não negativo, subtraído de 26, de modo a termos um múltiplo de 3 seria o 2.

### 3.2.2 Adição e resíduos após a divisão por 3

É muito importante entender como as operações aritméticas nos números inteiros afetam os restos.

Vamos investigar o que acontece quando os números são adicionados. Nosso objetivo é provar que o resíduo de uma soma é completamente definido pelos resíduos dos números que estão sendo adicionados (as parcelas).

Podemos verificar que, se dois números são divisíveis por 3, então sua soma é divisível por 3 também.

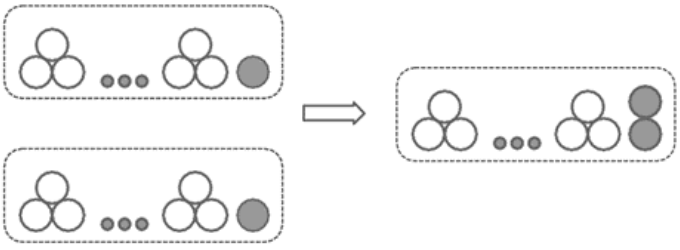
De fato, se $X = 3K$ e $Y = 3M$, então $X + Y = 3K + 3M = 3(K + M)$.

Agora, suponha que tanto $X$ quanto $Y$ tenham restos 1 quando divididos por 3. O que acontece com o resíduo da soma $X + Y$?

Antes de passar para a prova algébrica, vamos explicar a resposta usando um modelo visual.

Se um número inteiro não negativo tem resíduo 1, então é composto por vários grupos de 3 e um acréscimo de 1. Assim, quando dois desses números forem adicionados, a soma será composta por vários grupos de 3 e dos acréscimos, ou seja, 2. Então, a soma tem resto 2 (Figura 2).

Figura 2 – Soma composta por grupos divididos por 3 e resto 1 – Soma sem resto 2



Fonte: Elaborado pelos autores (2024)

Agora é hora de uma prova algébrica.

$$X = 3K + 1 \text{ e } Y = 3M + 1.$$

Portanto, $X + Y = 3K + 3M + 1 = 3(K + M) + 1 + 1 = 3(K + M) + 2$.

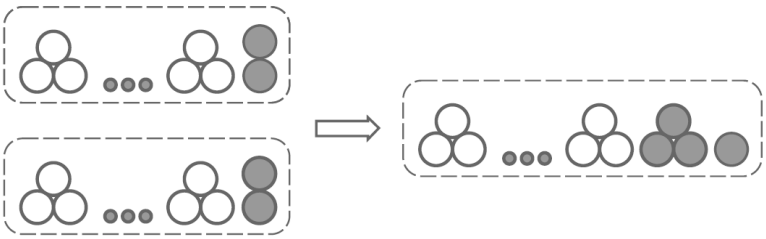
Assim, $X + Y$ tem resto 2.

Em seguida, suponha que **tanto** $X$ **quanto** $Y$ tenham **restos 2**. Qual seria o resto de $X + Y$? Vai ser 4 ou 1? Vamos provar:

$$X + Y = 3K + 2 + 3M + 2$$
$$= 3K + 3M + 2 + 2$$
$$= 3K + 3M + 3 + 1$$
$$= 3(K + M + 1) + 1.$$

Então, o resto é 1. Podemos ilustrar isso visualmente também, como expõe a Figura 3:

Figura 3 – Somas com resto 1



Fonte: Elaborado pelos autores (2024)

Vamos continuar analisando, temos várias outras combinações de restos para explorar. Para manter nossos resultados organizados, vamos criar uma tabela para esses resíduos. Temos condições de preencher uma tabela para a adição de resíduos. A tabela completa está abaixo:

Tabela 1 – Tabela completa de resíduos na divisão por 3

| + | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

Fonte: Elaborado pelos autores (2024)

Agora é hora de formular a regra geral de como os resíduos na divisão por 3 se comportam sob a adição.

Seria tentador dizer que os restos da soma de dois números é ***igual*** à soma de seus restos. Infelizmente, essa afirmação não é bem assim: dê uma olhada na Tabela 1, no par de restos (2, 2). Enquanto sua soma é 4, o resto de sua soma é 1.

- Assim, a regra correta no caso da divisão por 3 é: a soma de dois números tem o mesmo resíduo que o resíduo obtido na soma de seus respectivos resíduos.

- Aplicando o mesmo raciocínio, podemos chegar a uma regra semelhante para vários números na divisão por 3: a soma de vários números tem o mesmo resíduo que o resíduo obtido na soma de seus respectivos resíduos.

### 3.2.3 Multiplicação e restos após a divisão por 3

Vamos agora investigar o que acontece com os restos quando os números são multiplicados. O objetivo é provar que o resto de um produto é definido pelos restos dos fatores. Vamos provar caso a caso.

Podemos observar que, quando pelo menos **um dos dois termos é divisível por 3**, todo o produto é divisível por 3 também. De fato, suponha que X = 3*M* . Neste caso, *XY = (3M) Y = 3 (MY)*. Esse número é claramente divisível por 3.

Essa observação nos permite preencher algumas entradas na tabela de multiplicação de restos (Tabela 2):

Tabela 2 – Multiplicação de restos

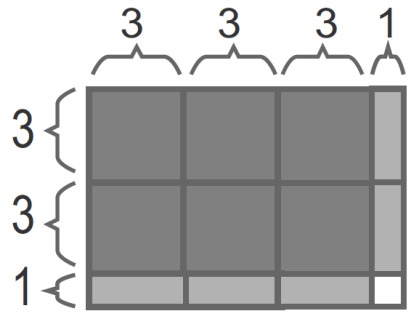
| × | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | | |
| 2 | 0 | | |

Fonte: Elaborado pelos autores (2024)

Em seguida, vamos **multiplicar dois números, cada um** tendo o resto **1**. O resto do produto será 1, e vamos provar esse fato de 2 maneiras: visualmente e algebricamente.

**Prova Visual:** Vamos utilizar o fato de que o produto de dois números pode ser visualizado como uma área de um retângulo, com lados iguais a estes números. A Figura 8 ilustra a multiplicação de dois números com restos 1. Cada um desses números contém vários grupos de 3 e um acréscimo de 1. Assim, o produto dos números é composto por vários quadrados $3 \times 3$ (cinza-escuro), vários retângulos $1 \times 3$ (cinza-claro), e um único quadrado $1 \times 1$ (branco). Todos quadrados $3 \times 3$ e todos os retângulos $1\times 3$ são múltiplos de 3. Portanto, o resto do produto é o quadrado branco $1 \times 1$, que tem uma área 1.

Figura 8 – Multiplicação de dois números com resto 1



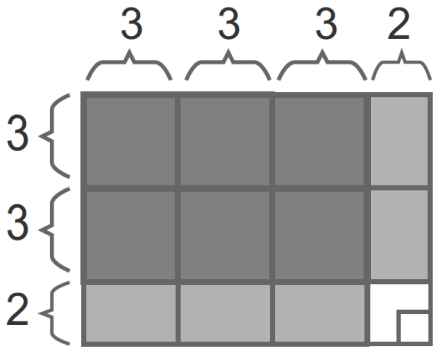

Fonte: Elaborado pelos autores (2024)

**A prova algébrica** demonstra a mesma ideia, expressa de forma mais compacta e formal:

$$(3M + 1) \cdot (3N + 1) = 3M \cdot 3N + 3M + 3N + 1$$
$$= 3\,(3M \cdot N + M + N\,) + 1.$$

Agora suponha que **cada um dos dois** números tenha **resto 2**. Qual seria o resto do produto? Mais uma vez, vamos começar com uma prova visual. A Figura 9 ilustra a multiplicação de dois números que tem restos 2. Da mesma forma que a prova anterior, cada quadrado cinza $3 \times 3$ é um múltiplo de 3, e cada retângulo cinza-claro $2 \times 3$ é um múltiplo de 3 também. Portanto, o resto é definido pelo quadrado branco $2 \times 2$. Três quadrados brancos $1 \times 1$ formam um múltiplo de 3 (em forma de L na figura). Assim, o resto é o quadrado branco $1 \times 1$, que tem uma área 1.

Figura 4 – Multiplicação de dois números com resto 2




Fonte: Elaborado pelos autores (2024)

Podemos seguir com uma prova algébrica:

$$(3M + 2) \cdot (3N + 2) = 3M \cdot 3N + 6M + 6N + 4$$
$$= 3(3M \cdot N + M + N + 1) + 1.$$

Da mesma forma, o produto dos dois números com os restos 1 e 2 terá resto 2.

Finalmente, podemos preencher toda a tabela de multiplicação.

Tabela 3 – Tabela de multiplicação

| × | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

Fonte: Elaborado pelos autores (2024)

Olhando para a Tabela 3, estamos prontos para formular a regra da multiplicação. Tal como no caso da adição, a alegação de que "o resto de um produto é igual ao produto dos restos" não é inteiramente verdadeira.

- A regra correta é: o produto de dois números tem o mesmo restante que o produto de seus restos. Isso vale para o produto de vários números.

## 4 RESULTADOS E ANÁLISES

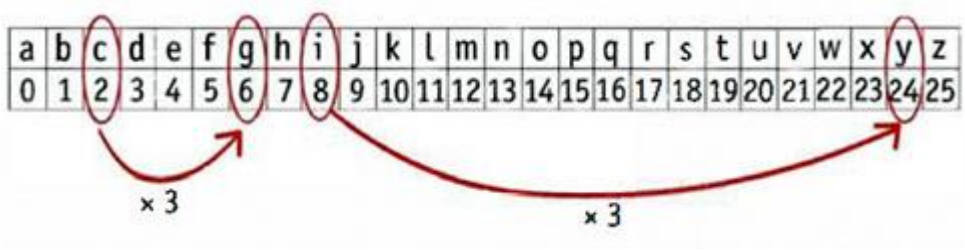
A frase "*resíduo (resto) quando dividido por...*" é um pouco longa. Matemáticos são um grupo que odeiam a fadiga, por isso eles sempre criam maneiras de encurtar as coisas – a notação "***módulo***" significa "o resto quando dividido". Por exemplo, a frase "o resto de 10, quando dividido por 3" pode ser substituída por "10 módulo 3", e a frase "5 tem resto 2 quando dividido por 3" pode ser substituída por "5 é igual a 2 módulo 3".

O símbolo especial de congruência "≡" pode ser usado para encurtar ainda mais as coisas e nos ajudar a não fazer mais uso da palavra "igual" que já está bem enraizada na teoria das equações. Por exemplo: "5 é igual a 2 módulo 3" pode ser reescrito como "5 é congruente a 2 módulo 3" e simbolizado por "$5 \equiv 2 (mod 3)$".

### 4.1 Cifras Multiplicativas

Vamos construir um método de criptografar chamado de *cifra 3-vezes*, onde se multiplica os números correspondentes às letras por 3 (veja a Tabela 4). Como exemplo, vamos encriptar a letra c. O número para c na tira é 2, multiplicando 2 por 3, obtemos 6. Como 6 é o número para a letra g, encriptamos c como g. Encriptamos a letra i como y porque o número para i é 8 e 3.8 = 24, e 24 corresponde a letra y.

Tabela 4 – Método de criptografar *cifra 3-vezes*




Fonte: Elaborado pelos autores (2024)

### 4.2 Chaves de Codificação

Ao aplicar as ideais propostas, professores e estudantes irão perceber que quando multiplicamos os números por 3, cada produto é diferente. Mas, quando multiplicarem por 2, algumas letras têm a mesma codificação. Portanto, multiplicar por 2 não é uma boa forma de cifragem.

Numa cifra multiplicativa, o número pelo qual se multiplica determina a cifra. Portanto, essa é a chave de codificação. Chamamos um número de uma boa chave se ele codifica cada letra de forma diferente. O número 3 é uma boa chave, mas o 2 não é. Uma questão a ser discutida é o que faz alguns números serem boas chaves, enquanto alguns números são chaves ruins.

- A regra geral é: *Um número é uma boa chave para uma cifra multiplicativa se for relativamente primo com o tamanho do alfabeto.*

### 4.3 Inversos Modulares

Encontrar inversos na Aritmética modular não é tão fácil como na Aritmética regular, mas há algumas formas de se fazer – algumas fáceis e outras não. É importante construir muitas tabelas para cifras multiplicativas (Tabela 5) e, assim, poder usar as suas tabelas para ajudar a encontrar outros inversos *mod* 26.

Tabela 5 – Letras multiplicadas pela *cifra 3-vezes*

| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 3 | 6 | 9 | 12 | 15 | 18 | 21 | 24 | **1** | 4 | 7 | 10 |
| **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
| 13 | 16 | 19 | 22 | 25 | 2 | 5 | 8 | 11 | 14 | 17 | 20 | 23 |

Fonte: Elaborado pelos autores (2024)

Por exemplo, acima temos a tabela da *cifra 3-vezes*. Temos os valores numéricos das letras que foram multiplicados por 3 e reduzidos *mod* 26. A Tabela 5 mostra que a letra J = 9 ficou com o valor $3 \times 9 \equiv 1\ (mod\ 26)$. Isso diz-nos que 3 e 9 são inversos *mod* 26.

## 5 CONSIDERAÇÕES FINAIS E CONTRIBUIÇÕES

Este artigo expôs propostas de atividades que usam Matemática para criptografar algumas das cifras clássicas e procuraram padrões em mensagens criptografadas que auxiliaram a decifrar as cifras usadas.

O texto inclui mais do que decifrar letras ou alterar o alfabeto. A criptografia requer Matemática como multiplicação, divisão com resto, fatores comuns e números primos. Também requer codificadores e decodificadores para criar e encontrar padrões, o que exigiu um nível mais profundo de pensamento.

Muitas pessoas têm a impressão errada de que a matemática é um assunto estático, no qual tudo é conhecido há centenas de anos. Assuntos como congruências e criptografia são como uma janela para as questões abertas e a natureza evolutiva da Matemática e, em particular, a Teoria dos Números, muitas vezes considerada um *playground* divertido para matemáticos, com pouca relevância para o mundo real. Neste artigo, quisemos mostrar que essas duas visões nunca foram um problema dentro da Matemática: diversão e aplicação.

## REFERÊNCIAS


BAILE, A. H. Recreations in the theory of numbers. 2nd revised ed. New York: Dover Publications, 1964.

BRASIL. Ministério da Educação. Secretaria de Educação Básica. **Base Nacional Comum Curricular**: educação é a base. Brasília, DF: MEC, 2015. Disponível em: http://basenacionalcomum.mec.gov.br. Acesso em: 9 jul. 2021.

BURTON, D. M. Teoria elementar dos números. Tradução de Gabriela dos Santos Barbosa. 7. ed. Rio de Janeiro: LTC, 2016.

CADAR, L. DUTENHEFNER, F. Encontros de Aritmética. Rio de Janeiro: IMPA/OBMEP, 2015.

DANTE, L. R. **Didática da resolução de problemas**. 12. ed. São Paulo: Ática, 2002.

MENDONÇA, M. do C. D. **Problematização**: um caminho a ser percorrido em educação matemática. 1993. 306 p. Tese (Doutorado em Educação) – Universidade Estadual de Campinas, Campinas, 1993. Disponível em: https://www.psiem.fe.unicamp.br/pf-psiem/domite_mariadocarmosantos_d.pdf. Acesso em: 30 jul. 2021.

SCHROEDER, T. L.; LESTER JR, F. K. Developing understanding in mathematics via problem solving. *In:* TRAFTON, P. R. (ed.). **New directions for elementary school mathematics**. Reston, VA: NCTM, 1989. p. 31-42.