# O Ensino de Aritmética Modular na Educação Básica

João Coelho Silva Filho [1]
UEMA, São Luís, MA.
Marcus Vinicius Viegas Rodrigues[2]
SEMED, Pinheiro, MA.

**Resumo**. O objetivo deste trabalho é mostrar a importância da Aritmética Modular para o ensino-aprendizagem de matemática. É evidenciado que há possibilidade de inserir objetos de conhecimento da Aritmética Modular nos organizadores curriculares da educação básica, segundo os documentos normativos, autores, pesquisadores e professores.Além disso, aborda-se a noção de Congruência apresentando diversos exemplos e aplicações no ensino, dando destaque à Aritmética dos Restos, aos Critérios de Divisibilidade, aos Dígitos Verificadores dos CPF, cartões de crédito, ao Calendário, entre outros.

**Palavras-chave**. Aritmética Modular, Aritmética dos Restos, Congruência.

## 1 Introdução

Neste trabalho, abordam-se situações que envolvem a Teoria dos Números, em especial a Aritmética Modular. Atualmente uma das ferramentas mais importantes na Teoria dos Números é a Aritmética Modular, pelo fato de envolver o conceito de Congruência, pois nos permite resolver diversas situações-problemas relacionadas à Divisibilidade, às Congruências Lineares, às Classes Residuais e às Equações Diofantinas Lineares.

A Aritmética modular tem muita aplicabilidade no cotidiano; no entanto, os organizadores curriculares do Ensino Básico contém apenas os conceitos e definições básicas de números naturais e suas operações, múltiplos, divisores, números primos, números compostos, regras de divisibilidade, máximo divisor comum, mínimo múltiplo comum e conceitos iniciais de números inteiros e suas operações. Estes tópicos são relacionados à Teoria dos Números, em especial, à Aritmética Modular que é muito mais ampla, e os livros didáticos deixam de abordar uma grande parte deles.

Há relatos sobre o Ensino de Aritmética Modular na Educação Básica, e embora os organizadores curriculares não detalhem os conteúdos dessa área, documentos normativos, autores, pesquisadores e professores defendem sua inclusão nos currículos.

## 2 Metodologia

Este trabalho apresenta uma pesquisa exploratória e descritiva, quanto ao procedimento, faz o uso primordialmente de pesquisa bibliográfica e, em alguns pontos, de pesquisa documental.

[1]coelhomat@uol.com.br
[2]marcus.vinicius.viegas.2015@gmail.com
[4]Este template foi baseado no modelo de trabalho completo do CNMAC 2024, disponível no Overleaf.

# 3 Resultados e Discussões

Diante das pesquisas na literatura específica, evidenciou-se que os conteúdos de Aritmética Modular não estão explicitamente dentre os objetos de conhecimentos propostos pelos documentos normativos da educação brasileira, tais como a Base Nacional Comum Curricular – BNCC e, de modo mais específico, o Documento Curricular do Território Maranhense – DCTMA.

Porém, segundo [6] por mais que não esteja de forma explícita nos currículos, a Aritmética Modular pode ser objeto de estudo na Educação Básica, não com o objetivo de ser apenas mais um conteúdo previsto, mas cada docente tem a possibilidade de atar aos objetos de conhecimento já presente nos organizadores curriculares.

Vale destacar, ainda, que [8] (p. 11) complementam que o ensino da Aritmética Modular na Educação Básica auxilia a consolidação do conceito de divisibilidade, proporciona que os alunos conheçam um contexto diferente para a realização das operações aritméticas e, ainda, incentiva um maior desenvolvimento do pensamento aritmético e sua ligação com o algébrico.

Outros autores defendem também a inserção da Aritmética Modular na educação básica, tais como [5] (p.13) ao argumentarem que ela pode auxiliar no desenvolvimento do pensamento matemático e na resolução de problemas. Segundo [7] (p.49), devido à importância do estudo e aplicabilidade das congruências modulares, que estimulam o desenvolvimento de habilidades essenciais para a formação do aluno, propõe-se o ensino de Congruências Modulares a partir do 6° ano do Ensino Fundamental.

Conforme a afirmação mencionada anteriormente de Ferreira [7] e diante do Organizador Curricular de Matemática do DCTMA,[6], nota-se que a inserção da Aritmética Modular pode ser feita, não apenas a partir do 6° ano, mas desde o 5° ano do Ensino Fundamental, visto que há possibilidade de fazer a relação dela com alguns objetos de conhecimento de algumas habilidades desse ano e de anos posteriores.

Constata-se que, no Ensino Fundamental do 5° ao 7° ano, há possibilidade da inserção da noção de congruência no componente curricular Matemática. Note que a habilidade número 10 do 5° ano da BNCC tem como objeto de conhecimento “Propriedades da igualdade e noção de equivalência”, desse modo é pertinente abordar a simbologia de congruência $\equiv$ como uma noção de equivalência enfatizando suas propriedades.

Essa noção vai ser aprofundada no 6° ano, visto que as habilidade número 05 e 06 possuem como objetos de conhecimento “Múltiplos e Divisores de um número natural; Números primos e compostos". Percebe-se que os alunos terão um contato mais acentuado com os critérios de divisibilidade, o que é uma excelente oportunidade para aprofundar a noção de congruência, já que é uma nova maneira de se comparar os números naturais. Por exemplo, dividindo uma turma de 31 alunos em dois grupos, de modo que um grupo A tenha 14 alunos e um grupo B tenha 17, e consequentemente fizermos uma nova divisão dentro de cada grupo formando subgrupos de 3 alunos, notaremos que ambos os grupos terão 2 alunos sobrando. Assim, tem-se que 14 e 17 são congruentes módulo 3, pois quando divididos por 3, o resto é o mesmo.

Consequentemente, ao encontro com a habilidade número 01 do 7°ano, cujo objeto de conhecimento é “Múltiplos e divisores de um número natural”, a noção de congruência modular pode ser retomada. Nesse mesmo ano, essa noção pode ser aprofundada conforme a habilidade número 04, em que o objeto de conhecimento é “Números inteiros: usos, história, ordenação, associação com pontos da reta numérica e operações”, pois ampliaremos a noção para o conjunto dos números inteiros.

[1] (p.67) propõe o estudo de congruências no Ensino Médio. Com o mesmo objetivo, [2] (p.05) acredita que esse objeto de estudo, quando aplicado nesse nível de ensino, pode desenvolver nos alunos habilidades que lhes pertimem criar conjecturas, tornando-os mais à vontade para fazer abstrações e estimulando argumentações, tanto orais quanto escritas, em diferentes níveis. Assim, com base no que foi exposto, pode-se inferir que o ensino da Aritmética Modular também pode

ser alinhado ao currículo do ensino médio.

## 3.1 Aritmética Modular

Consoante [4], o algoritmo da divisão de Euclides é um resultado importante da Teoria dos Números e também no fundamento das Congruências.

**Algoritmo da Divisão de Euclides.** Considere dois inteiros $a$ e $b$, com $b \neq 0$, então existem únicos inteiros $q$ e $r$ tais que

$$a = qb + r, \text{ com } 0 \leq r <\mid b \mid .$$

Os inteiros $q$ e $r$ são denominados, respectivamente, de quociente e resto, e $r = 0$ se, e somente se, $b$ é divisor de $a$ ou $b$ divide $a$, em símbolo: $b \mid a$.

**Definição 3.1.** Sejam $a$ e $b$ dois inteiros não nulos. O máximo divisor comum de $a$ e $b$ é o inteiro positivo $d$ que satisfaz às seguintes condições:

1. $d \mid a$ e $d \mid b$;
2. Se $c \mid a$ e se $c \mid b$, então $c \leq d$.

O máximo divisor comum de $a$ e $b$ é indicado por: $d = mdc(a, b)$. É imediato que $mdc(a, b) = mdc(b, a)$.

**Definição 3.2.** [Congruência]
Dois inteiros $a$ e $b$ são congruentes módulo $n$, n inteiro positivo maior que 1, se os restos da divisão de $a$ e de $b$ por $n$ são iguais. Em símbolo, $a \equiv b \bmod n$.

Tem-se algumas propriedades das Congruências: considere $a$ e $b$ inteiros, $a \equiv b \bmod n$ se, e somente se, $n \mid (a - b)$. Logo,

**i-** $a \equiv a \bmod n$ para todo $a \in \mathbb{Z},\ n \in \mathbb{N}$ e $n > 1$;

**ii-** $a \equiv b \bmod n \Rightarrow b \equiv a \bmod n$ para todo $a,\ b \in \mathbb{Z}$;

**iii-** $a \equiv b \bmod n$ e $b \equiv c \bmod n \Rightarrow a \equiv c \bmod n$ para todo $a,\ b,\ c \in \mathbb{Z}$;

**iv-** $a \equiv b \bmod n$ e $c \equiv d \bmod n \Rightarrow (a + c) \equiv (b + d) \bmod n$ para todo $a,\ b,\ c,\ d \in \mathbb{Z}$;

**v-** $a \equiv b \bmod n$ e $c \equiv d \bmod n \Rightarrow (a \cdot c) \equiv (b \cdot d) \bmod n$ para todo $a,\ b,\ c,\ d \in \mathbb{Z}$;

**vi-** $a \equiv b \bmod n \Rightarrow a^k \equiv b^k \bmod n$ para todo $a,\ b \in \mathbb{Z},\ k \in \mathbb{N}$.

Conforme [3],a Congruência e suas propriedades são de grande utilidade na resolução de problemas e são a ferramenta para justificar os critérios de divisibilidade mnemônicas, o calendário, os dígitos verificadores de CPF, cartão de crédito, entre outros.

## 3.2 Aplicações de Aritmética Modular no Ensino

### 3.2.1 Critérios de Divisibilidade

Um numéro inteiro $N = n_r n_{r-1} n_{r-2} \cdots n_2 n_1 n_0$ pode ser escrito na base decimal como:

$$N = n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + n_{r-2} \cdot 10^{r-2} + \cdots n_2 \cdot 10^2 + n_1 \cdot 10^1 + n_0 \cdot 10^0,$$

em que os números $n_i \in \{0, \cdots, 9\}$ são chamados de dígitos de $N$.

Desse modo, serão utilizados os conceitos e propriedades das Congruências para definir alguns critérios de divisibilidade.

**Divisibilidade por 2**

Utilizando a noção de congruência, note que $10 \equiv 0 \ mod\ 2$, segue-se do item 3 das propriedades das Congruências que

$$10^i \cdot n_i \equiv 0 \ mod\ 2,$$

para algum $i \geq 1$. Portanto,

$$N = n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + n_{r-2} \cdot 10^{r-2} + \cdots + n_2 \cdot 10^2 + n_1 \cdot 10^1 + n_0 \cdot 10^0$$

$$N = 10 \cdot (n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \cdots + n_2 \cdot 10^1 + n_1 \cdot 10^0) + n_0$$

$$N = 10 \cdot (n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \cdots + n_2 \cdot 10^1 + n_1 \cdot 10^0) + n_0 \equiv \ 0 \ mod\ 2,$$

assim,

$$N \equiv \ n_0 \ mod\ 2.$$

Logo $N$ é divisível por 2 se, e somente se, $n_0$ é divisível por 2, ou seja, se $n_0$ for par.

**Divisibilidade por 3 e 9**

Utilizando a noção de congruência, note que $10 \equiv 1 \ mod\ 3 \quad e \quad 10 \equiv 1 \ mod\ 9$, segue-se do item 3 das propriedades das Congruências que

$$10^i \equiv 1 \ mod\ 3 \quad e \quad 10^i \equiv 1 \ mod\ 9$$

para $i \geq 1$.

Isso mostra que se,

$$N = n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + n_{r-2} \cdot 10^{r-2} + \cdots + n_2 \cdot 10^2 + n_1 \cdot 10^1 + n_0 \cdot 10^0$$

então, $N \equiv (n_r + n_{r-1} + n_{r-2} + \cdots n_2 + n_1 + n_0) \ mod\ 3 \quad e \quad N \equiv (n_r + n_{r-1} + n_{r-2} + \cdots n_2 + n_1 + n_0) \ mod\ 9$. Um número inteiro $N$ é divisível por 3 quando a soma de seus algarismos é divisível por 3. E por 9 quando a soma de seus algarismos também é divisível por 9.

**Divisibilidade por 6**

Um número inteiro $N$ é divisível por 6 quando é divisível por 2 e 3 simultaneamente. Uma justificativa desse critério vem do Teorema Fundamental da Aritmética que afirma que todo número inteiro maior que 1 pode ser escrito de maneira única como um produto de números primos, desconsiderando a ordem dos fatores. A partir dele obtém-se a decomposição em fatores primos do 6, que $6 = 2 \cdot 3$.

**Divisibilidade por 4 e 8**

Utilizando a noção de congruência, note que $10 \equiv 2 \ mod\ 4 \quad e \quad 10 \equiv 2 \ mod\ 8$, segue-se do item 3 das propriedades das Congruências, $10^2 \equiv 2^2 \equiv 0 \cdot 1 \ mod\ 4$, da mesma forma, $10^3 \equiv 2^3 \equiv 1 \cdot 0 \cdot 1 \ mod\ 4$, de modo análogo $10^3 \equiv 2^3 \equiv 0 \ mod\ 8$ o que implica em

$$10^i \equiv 0 \ mod\ 4 \quad e \quad 10^k \equiv 0 \ mod\ 8$$

para $i \geq 2$ e $k \geq 3$.

Isso mostra que, se

$$N = n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + n_{r-2} \cdot 10^{r-2} + \cdots + n_2 \cdot 10^2 + n_1 \cdot 10^1 + n_0 \cdot 10^0,$$

então

$$N \equiv 0 + 0 + 0 + \cdots + 10^1 \cdot n_1 + n_0 \ mod\ 4 \quad e \quad N \equiv 0 + 0 + 0 + \cdots + 0 + n_2 n_1 n_0 \ mod\ 8.$$

Logo, $N$ é divisível por 4 se, e somente se, $10^1 \cdot n_1 + n_0$, ou seja, $n_1 n_0$ é divisível por 4. Um número inteiro $N$ é divisível por 4 quando seus dois últimos algarismos formam um número divisível por 4, ou seja, $N \equiv (2n_1 + n_0)\ mod\ 4$.
De modo análogo, $N$ é divisível por 8 se, e somente se, $10^2 \cdot n_2 + 10^1 \cdot n_1 + n_0$, ou seja, $n_2 n_1 n_0$ é divisível por 8. Assim, um número inteiro $N$ é divisível por 8 se, e somente se, quando termina em 000 ou quando os últimos três algarismos da direita for divisível por 8.

**Divisibilidade por 5**

Utilizando a noção de congruência, note que $10 \equiv 0\ mod\ 5$, segue-se do item 3 das propriedades das Congruências, o que implica em

$$10^i \equiv 0\ mod\ 5,$$

para $i \geq 1$.

Isso mostra que, se

$$N = n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + n_{r-2} \cdot 10^{r-2} + \cdots + n_2 \cdot 10^2 + n_1 \cdot 10^1 + n_0 \cdot 10^0$$

então

$$N \equiv 0 + 0 + 0 + \cdots + n_0\ mod\ 5.$$

Logo, $N$ é divisível por 5 se, e somente se, $n_0$ é divisível por 5, ou seja, se $n_0$ for 0 ou 5.

## 3.3 Dígito Verificador CPF

O Cadastro de Pessoa Física (CPF) é um conjunto de números que serve para identificação de uma pessoa. O cadrasto possui 11 dígitos, dos quais o nono dígito identifica o estado brasileito de emissão da pessoa. Os dois últimos números são dígitos verificadores (ou de controle), sendo essa mais uma aplicação de congruência, que utiliza congruência módulo 11, operando com os nove primeiros algarismos:

$$c = [\ a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8\ a_9\ ]$$

e esses algarismos ficam sendo multiplicados, conforme a ordem dada no documento, pela primeira matriz de pesos pré-estabelecida em CPF's por:

$$p = [\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ ].$$

Assim, é feito o produto matricial entre $c$ e $p^t$, dando uma soma ($S$) e a congruência usada é:

$$S - a_{10} \equiv 0\ mod\ 11,$$

$$a_{10} \equiv S\ mod\ 11 \quad ou \quad S \equiv a_{10}\ mod\ 11.$$

Para encontrar o segundo dígito verificador o mesmo processo é realizado, todavia acrescentando $a_{10}$ em $c$ e a matriz $p$ passa a ser:

$$p = [\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ ].$$

Em outras palavras, o decimo dígito, ou primeiro verificador é calculado assim: multiplica-se o primeiro número por 1, o segundo por 2, o terceiro por 3, até o nono que deve ser multiplicado por 9. Soma-se os resultados obtidos e calcula-se o resto da divisão por 11, tal resto será o primeiro dígito de controle, exceto se tal resto for 10, situação em que o dígito será 0. Para o segundo dígito de controle multiplica-se o segundo número por 1, o terceiro por 2, o quarto por 3 até o décimo número que deve ser multiplicado por 9, soma-se os resultados obtidos e divide-se por 11, o segundo dígito de controle é o resto dessa divisão. Como antes, se tal resto for 10, o dígito verificador será 0.

**Exemplo 4.1.** *Encontre os dígitos verificadores do CPF fictício dado por*: **515.253.545-** $a_{10}a_{11}$.
*Solução:* Para encontrar o primeiro dígito, faz-se o produto das matrizes:

$c_1 = [\ 5\ 1\ 5\ 2\ 5\ 3\ 5\ 4\ 5\ ]$ e $p_1 = [\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ ]$,

assim, obtém-se a soma $(S)$ em cada caso:

$$S_1 = 5 \cdot 1 + 1 \cdot 2 + 5 \cdot 3 + 2 \cdot 4 + 5 \cdot 5 + 3 \cdot 6 + 5 \cdot 7 + 4 \cdot 8 + 5 \cdot 9$$

$$S_1 = 5 + 2 + 15 + 8 + 25 + 18 + 35 + 32 + 45$$

$$S_1 = 5 + 2 + 15 + 8 + 25 + 18 + 35 + 32 + 45$$

$$S_1 = 185.$$

Logo,

$$S_1 - a_{10} \equiv 0\ mod\ 11$$

$$185 - a_{10} \equiv 0\ mod\ 11.$$

Portanto, $a_{10}$ é igual a 9.

Agora, para calcular o último dígito, toma-se

$c_2 = [\ 5\ 1\ 5\ 2\ 5\ 3\ 5\ 4\ 5\ 9\ ]$ e $p_1 = [0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ ]$.

Assim, encontra-se a outra soma:

$$S_2 = 5 \cdot 0 + 1 \cdot 1 + 5 \cdot 2 + 2 \cdot 3 + 5 \cdot 4 + 3 \cdot 5 + 5 \cdot 6 + 4 \cdot 7 + 5 \cdot 8 + 9 \cdot 9$$

$$S_2 = 0 + 1 + 10 + 6 + 20 + 15 + 30 + 28 + 40 + 81$$

$$S_2 = 231.$$

Mas, como

$$S_2 - a_{11} \equiv 0\ mod\ 11,$$

tem-se que

$$231 - a_{11} \equiv 0\ mod\ 11.$$

Logo, $a_{11} = 0$, e o CPF será **515.253.545-90**.

## 3.4 Calendário

Quando se trata de calendário, nota-se que há um grande enredo matemático por trás. Utilizando congruência modulo m, com $m = 7$ no calendário, referente ao mês de julho de 2024, observa-se que

*Domingo* : $n \equiv 0\ mod\ \mathbf{7}$; *Segunda* : $n \equiv 1\ mod\ \mathbf{7}$; $Terca$ : $n \equiv 2\ mod\ \mathbf{7}$; *Quarta* : $n \equiv 3\ mod\ \mathbf{7}$; *Quinta* : $n \equiv 4\ mod\ \mathbf{7}$; *Sexta* : $n \equiv 5\ mod\ \mathbf{7}$; *Sabado* : $n \equiv 6\ mod\ \mathbf{7}$.

Para determinar, por exemplo, qual dia da semana seria 30 de julho de 2024, bastaria apenas saber a que classe de congruência que esse dia pertenceria em módulo 7. Dessa forma, dividindo 30 por 7. resulta em um quociente 4 e resto 2. Assim, $30 \equiv 2\ mod\ 7$, ou seja, sabe-se que segunda-feira é a data inicial do mês, dia 1, a classe de restos 2 pertence nesse sentindo às terças-feiras. Portanto, dia 30 de julho de 2024 é terça-feira.

# 4 Considerações Finais

Compreende-se que a importância da Aritmética Modular no ensino é extraordinária e totalmente relevante. Por mais que não esteja presente nos currículos do ensino básico, os docentes de matemática podem inserir, consoante a documentos educacionais, em suas aulas esse conteúdo, desde que atrelados aos conteúdos de Teoria dos Números contidos nas grades curriculares. Isso se dá pelo fato da Aritmética Modular trazer um rol de aplicações de fácil compreensão pelos alunos da educação básica, tais como à divisibilidade, ao calendário, ao relógio, ao CPF, aos cartões de crédito, entre outros.

# Referências


[1] GOMES Ataniel Rogério Gonçalves et al. **Uma abordagem do ensino de congruência na educação básica**. 2015. 76p. Dissertação (Mestrado em Matemática)-UFS, Itabaiana- SE, 2015.

[2] OLIVEIRA Elizabeth Magalhães, PINTO Marco Antonio di, SILVA Marcia Roberta Santos Pires da e COSTA Michel da. "UMA PROPOSTA DE ENSINO DE ARITMÉTICA MODULAR PARA EDUCAÇÃO BÁSICA". Em: **VII CONGRESSO INTERNACIONAL DE ENSINO DE MATEMÁTICA-2017**. 2017.

[3] LEITÃO Filliphe de A. **Aritmética modular e suas aplicações: uma experiência de atuação no Ensino Básico**. 2019. 77p. Dissertação (Mestrado em Matemática)-UEMA, São Luís-MA, 2019.

[4] COELHO J. e LEITÃ0. F. de A. **Aritmética Modular Aplicada aos Critérios de Divisibilidade Mnemônicos e Não Mnemônicos, Ebook Formando Docentes Construindo Saberes, PROFMAT-UEMA**. 2021.

[5] SILVA Luciano M. e PONTES. Edel Alexandre Silva. "Aritmética Modular como proposta de ensino de Matemática: uma experiência prática em uma Escola Pública de ensino fundamental". Em: **Revista Diálogos em Educação Matemática** 2.1 (2023), e202304–e202304.

[6] RODRIGUES M. V. V. **Aritmética Modular Aplicada**. 2024. 72p. Dissertação (Mestrado em Matemática)-UEMA, São Luís-MA, 2024.

[7] FERREIRA Rosiane Barros et al. **Congruência modular no ensino básico.** 2018. 46p. Dissertação (Mestrado em Matemática)-UFMA, São Luís-MA, 2018.

[8] MATTOS. S. R. P., PUGGIAN C. e LOZANO. A. G. "Aritmética Modular E Suas Possibilidades Na Formação Continuada De Professores De Matemática (CO)". Em: **XIII CONFERÊNCIA INTERAMERICANA DE EDUCAÇÃO MATEMÁTICA**. 2011.