ReGeo ISSN: 2177-3246

CRITÉRIOS DE DIVISIBILIDADE COMO AVALIAÇÃO MODULAR DA REPRESENTAÇÃO POSICIONAL

DIVISIBILITY CRITERIA AS MODULAR EVALUATIONS OF POSITIONAL REPRESENTATION

CRITERIOS DE DIVISIBILIDAD COMO EVALUACIONES MODULARES DE LA REPRESENTACIÓN POSICIONAL

https://doi.org/10.56238/revgeov17n7-072

Data de submissão: 30/05/2026 **Data de publicação:** 14/07/2026

Alberdan Rafael Carneiro de Vasconcelos
Graduado em Licenciatura em Matemática
Instituição: Universidade Federal da Paraíba
E-mail: profalberdanvasconcelos@gmail.com

RESUMO

Este artigo analisa critérios de divisibilidade como consequências da representação posicional dos inteiros e da avaliação modular de polinômios. O objetivo é organizar critérios conhecidos em uma formulação comum, distinguindo regras que preservam o resto, regras que preservam apenas a divisibilidade e simplificações obtidas por propriedades da base em relação ao divisor. A pesquisa adota abordagem bibliográfica e teórico-dedutiva, com revisão de literatura, formalização algébrica, demonstração por congruências e comparação entre critérios clássicos, critérios por blocos, critérios por unidades modulares e a recorrência do método de Horner. Os resultados são apresentados em três níveis de generalidade: a forma geral do argumento, um exemplo genérico com base, divisor e algarismos arbitrários, e exemplos numéricos em bases distintas. Mostra-se que a soma dos algarismos, a soma alternada, os critérios pelos últimos algarismos e a soma de blocos são casos particulares da avaliação modular da escrita posicional. O trabalho não reivindica a criação de um critério universal inédito; sua contribuição consiste em classificar esses procedimentos, explicitar suas hipóteses e indicar o que cada transformação conserva.

Palavras-chave: Divisibilidade. Congruência Modular. Método de Horner. Representação Posicional. Teoria dos Números.

ABSTRACT

This article analyzes divisibility criteria as consequences of positional representation of integers and modular evaluation of polynomials. The objective is to organize known criteria in a common formulation, distinguishing rules that preserve the remainder, rules that preserve only divisibility, and simplifications obtained by properties of the base in relation to the divisor. The research adopts a bibliographic and theoretical-deductive approach, with literature review, algebraic formalization, demonstration by congruences, and comparison between classical criteria, block criteria, modular unit criteria, and the recurrence of Horner's method. The results are presented at three levels of generality: the general form of the argument, a generic example with arbitrary base, divisor, and digits, and numerical examples in distinct bases. It is shown that the sum of digits, alternating sum, criteria for last digits, and sum of blocks are special cases of modular evaluation of positional representation. The work does not claim the creation of an original universal criterion; its contribution consists of classifying these procedures, making their hypotheses explicit, and indicating what each transformation preserves.

Keywords: Divisibility. Modular Congruence. Horner's Method. Positional Representation. Number Theory.

RESUMEN
Este artículo analiza los criterios de divisibilidad como consecuencias de la representación posicional de números enteros y la evaluación modular de polinomios. El objetivo es organizar criterios conocidos en una formulación común, distinguiendo reglas que preservan el resto, reglas que preservan solo la divisibilidad y simplificaciones obtenidas por propiedades de la base en relación al divisor. La investigación adopta un enfoque bibliográfico y teórico-deductivo, con revisión de literatura, formalización algebraica, demostración por congruencias y comparación entre criterios clásicos, criterios por bloques, criterios por unidades modulares y la recurrencia del método de Horner. Los resultados se presentan en tres niveles de generalidad: la forma general del argumento, un ejemplo genérico con base, divisor y dígitos arbitrarios, y ejemplos numéricos en bases distintas. Se demuestra que la suma de dígitos, suma alternada, criterios por últimos dígitos y suma de bloques son casos particulares de la evaluación modular de la representación posicional. El trabajo no reclama la creación de un criterio universal original; su contribución consiste en clasificar estos procedimientos, hacer explícitas sus hipótesis e indicar qué conserva cada transformación.

Palabras clave: Divisibilidad. Congruencia Modular. Método de Horner. Representación Posicional. Teoría de Números.

1 INTRODUÇÃO

Os critérios de divisibilidade aparecem com frequência no ensino básico como regras independentes: somar os algarismos para testar a divisibilidade por 3 ou por 9, alternar somas para testar a divisibilidade por 11, ou observar os últimos algarismos para testar a divisibilidade por potências de 2 e de 5. Essa apresentação é útil para o cálculo mental, mas costuma ocultar a estrutura algébrica comum a todos esses procedimentos: cada um deles avalia, módulo o divisor, o polinômio determinado pelos algarismos do número.

A literatura matemática e computacional já contém formulações gerais para critérios de divisibilidade. Grinberg e Luryi (2014) apresentam uma formulação geral em bases arbitrárias, na qual o teste é expresso por combinações lineares dos dígitos com pesos determinados pela base e pelo divisor. Pereira e Ribas (2025) constroem, na base decimal, critérios para divisores inteiros, usando congruências e a ordem de 10 módulo d quando essa ordem está definida. Sutner (2010) aproxima a divisibilidade da leitura sequencial dos dígitos, por meio de autômatos associados à recorrência de Horner, enquanto Alexeev (2004) examina a minimalidade dos autômatos finitos usados no teste de divisibilidade. Neste artigo, esses resultados são retomados para classificar os critérios segundo a informação que cada procedimento conserva: o resto, apenas a divisibilidade, ou uma simplificação por agrupamento.

O problema investigado é: como os critérios clássicos e gerais de divisibilidade podem ser descritos como casos particulares da avaliação modular da representação posicional, e em que sentido a recorrência de Horner fornece uma forma iterativa de calcular classes de congruência preservando o resto original?

O artigo mostra que a escrita posicional de um inteiro pode ser interpretada como a avaliação de um polinômio na base do sistema de numeração. Nessa perspectiva, trocar a base b por qualquer inteiro com o mesmo resto módulo d não altera a classe de congruência do número analisado. A recorrência de Horner transforma essa ideia em um procedimento iterativo, capaz de calcular a classe de congruência sem desenvolver as potências da base.

O texto está organizado da seguinte forma. A Seção 2 apresenta a fundamentação teórica: representação posicional, congruência modular e o método de Horner. A Seção 3 descreve a metodologia. A Seção 4 desenvolve os resultados em três níveis de generalidade — a forma geral do argumento (Proposição 1), um exemplo genérico com dados arbitrários e dois exemplos numéricos em bases distintas — e, em seguida, deriva os critérios clássicos, os critérios por blocos e os critérios por unidades modulares como casos particulares. A Seção 5 apresenta as considerações finais.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 REPRESENTAÇÃO POSICIONAL E POLINÔMIO DOS DÍGITOS

Seja $b \geq 2$ um inteiro fixado, chamado base do sistema de numeração. Todo inteiro positivo N admite uma única representação na base b da forma

$$N = (a_m a_{m-1} \cdots a_1 a_0)_b = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0 = \sum_{k=0}^{m} a_k b^k, \quad (1)$$

em que os algarismos satisfazem $0 \leq a_k < b$ para todo $0 \leq k \leq m$, com $a_m \neq 0$ (KNUTH, 1997). Essa escrita associa a N o polinômio dos dígitos

$$P(x) = \sum_{k=0}^{m} a_k x^k, \quad (2)$$

de modo que $N = P(b)$. Estudar a divisibilidade de N por um inteiro $d > 1$ equivale, portanto, a estudar o valor de $P(b)$ módulo d .

Recorde-se a definição de congruência. Dados $a, c \in Z$, diz-se que a é congruente a c módulo d , e escreve-se $a \equiv c \pmod{d}$, quando d divide a diferença $a - c$, isto é,

$$a \equiv c \pmod{d} \Leftrightarrow d \mid (a - c) \Leftrightarrow \exists q \in Z : a - c = qd. \quad (3)$$

De forma equivalente, $a \equiv c \pmod{d}$ se, e somente se, a e c deixam o mesmo resto na divisão euclidiana por d : existem $q_1, q_2 \in Z$ e $0 \leq r < d$ tais que

$$a = q_1 d + r, \; c = q_2 d + r. \quad (4)$$

A utilidade da congruência para os critérios de divisibilidade decorre de sua compatibilidade com as operações aritméticas, registrada no lema a seguir (MARTINEZ *et al.*, 2018).

Lema 1 (compatibilidade com soma e produto). Sejam $a, a', c, c' \in Z$ e $d > 1$. Se $a \equiv a' \pmod{d}$ e $c \equiv c' \pmod{d}$, então

$$a + c \equiv a' + c' \pmod{d} \; e \; ac \equiv a'c' \pmod{d}. \quad (5)$$

Demonstração. Por hipótese, existem $q_1, q_2 \in Z$ tais que $a - a' = q_1 d$ e $c - c' = q_2 d$. Para a soma, $(a + c) - (a' + c') = (q_1 + q_2) d$, que é múltiplo de d . Para o produto,

$$ac - a'c' = a(c - c') + c'(a - a') = (a q_2 + c' q_1) d, \quad (6)$$

que também é múltiplo de d . ∎

O Lema 1 autoriza substituir, em qualquer soma ou produto, cada parcela ou fator por outro inteiro congruente, sem alterar a classe de congruência do resultado. É exatamente essa liberdade que os critérios de divisibilidade exploram.

2.2 SUBSTITUIÇÃO DA BASE MÓDULO D

Lema 2 (substituição da base). Sejam $b \geq 2$, $d > 1$ e $u \in Z$ com $u \equiv b \pmod{d}$. Então $u^k \equiv b^k \pmod{d}$ para todo inteiro $k \geq 0$ e, consequentemente,

$$N = \sum_{k=0}^{m} a_k b^k \equiv \sum_{k=0}^{m} a_k u^k = P(u) \pmod{d}. \tag{7}$$

Demonstração. A primeira afirmação segue por indução sobre k . Para $k = 0$, tem-se $u^0 = 1 = b^0$, e a congruência é imediata. Suponha $u^k \equiv b^k \pmod{d}$ para algum $k \geq 0$. Como $u \equiv b \pmod{d}$, a parte multiplicativa do Lema 1 fornece

$$u^{k+1} = u^k \cdot u \equiv b^k \cdot b = b^{k+1} \pmod{d}. \tag{8}$$

Para a segunda afirmação, aplica-se o Lema 1 a cada parcela — $a_k b^k \equiv a_k u^k \pmod{d}$ — e, em seguida, à soma das parcelas. ∎

Consequentemente,

$$d \mid N \Leftrightarrow P(u) \equiv 0 \pmod{d}. \tag{9}$$

Essa é a forma elementar da avaliação modular da escrita posicional: u pode ser escolhido como qualquer representante da classe de b módulo d — em particular, um representante de valor absoluto pequeno, o que simplifica os cálculos.

2.3 CRITÉRIOS GERAIS DE DIVISIBILIDADE NA LITERATURA

Grinberg e Luryi (2014) formulam critérios universais como formas lineares nos dígitos do número, em qualquer base. O ponto comum com a formulação adotada neste artigo é o uso de pesos modulares associados às potências da base. Pereira e Ribas (2025) constroem critérios na base decimal por meio de congruências e, nos casos coprimos, pela ordem de 10 módulo d , obtendo critérios por blocos quando alguma potência de 10 é congruente a 1 módulo d .

Essas abordagens mostram que critérios gerais de divisibilidade já estão presentes na literatura. O foco deste trabalho não é propor outro critério universal, mas explicitar como critérios clássicos, critérios por blocos e critérios por unidades modulares podem ser lidos como transformações de uma mesma avaliação posicional.

2.4 MÉTODO DE HORNER E CÁLCULO ITERATIVO DA CLASSE MODULAR

O método de Horner (HORNER, 1819; KNUTH, 1997) reescreve o polinômio dos dígitos em forma aninhada:

$$P(u)=(\cdots(a_m u+a_{m-1})u+a_{m-2})u+\cdots+a_1)u+a_0. \tag{10}$$

Essa forma dispensa o cálculo separado das potências de u : cada etapa usa apenas uma multiplicação e uma adição. Definindo a recorrência

$$r_0=a_m, r_i \equiv r_{i-1}u+a_{m-i}\,(\mathrm{mod}\,d), 1\le i\le m, \tag{11}$$

obtém-se, ao final, $r_m \equiv P(u) \equiv N\,(\mathrm{mod}\,d)$.

A recorrência calcula um representante da classe de congruência de N módulo d . Se esse representante for reduzido ao conjunto $\{0,1,\ldots,d-1\}$, obtém-se o resto da divisão euclidiana de N por d . Essa distinção é importante: um valor congruente ao resto não é, em geral, o próprio resto.

3 METODOLOGIA

A pesquisa é bibliográfica e teórico-dedutiva. O procedimento não envolve coleta empírica de dados; trabalha-se com definições, proposições, demonstrações por congruência modular e exemplos numéricos. A análise parte da escrita de um inteiro como polinômio na base b , reduz essa base módulo d , aplica a recorrência de Horner e compara os critérios obtidos quanto à propriedade que preservam: o resto, apenas a divisibilidade, ou a dependência de blocos finais.

A exposição dos resultados segue três níveis de generalidade, do abstrato ao concreto: primeiro, a forma geral do argumento, enunciada e demonstrada como proposição; em seguida, um exemplo genérico, no qual base, divisor e algarismos permanecem arbitrários e a recorrência é executada simbolicamente; por fim, exemplos numéricos em bases distintas, que ilustram a independência do procedimento em relação à base decimal. Essa organização evita tratar critérios de divisibilidade como uma coleção de regras isoladas: o mesmo formalismo explica critérios tradicionais, critérios obtidos pela ordem da base e critérios que usam inversos modulares.

4 RESULTADOS E DISCUSSÃO

4.1 A FORMA GERAL DO ARGUMENTO

O argumento central pode ser descrito em três passos. Primeiro, escreve-se N na base b, o que o identifica com o valor $P(b)$ do polinômio dos dígitos. Segundo, escolhe-se $u \equiv b \pmod{d}$, de preferência com valor absoluto pequeno; pelo Lema 2, $N \equiv P(u) \pmod{d}$. Terceiro, avalia-se $P(u)$ módulo d pela recorrência de Horner, reduzindo cada etapa módulo d sempre que conveniente. A proposição a seguir formaliza o esquema.

Proposição 1. Seja $N = (a_m a_{m-1} \cdots a_0)_b$, com $b \geq 2$, e seja $d > 1$. Se $u \equiv b \pmod{d}$, então a recorrência

$$r_0 = a_m,\ r_i \equiv r_{i-1} u + a_{m-i} \pmod{d},\ 1 \leq i \leq m, \tag{12}$$

produz um valor r_m tal que $r_m \equiv N \pmod{d}$.

Demonstração. Afirma-se que, para todo $0 \leq i \leq m$,

$$r_i \equiv a_m u^i + a_{m-1} u^{i-1} + \cdots + a_{m-i} \pmod{d}. \tag{13}$$

Para $i = 0$, a definição fornece $r_0 = a_m$, e a afirmação vale trivialmente. Suponha-a válida para algum i com $0 \leq i < m$. Pela definição da recorrência e pela compatibilidade da congruência com soma e produto (Lema 1),

$$r_{i+1} \equiv r_i u + a_{m-i-1} \equiv (a_m u^i + \cdots + a_{m-i}) u + a_{m-i-1} \pmod{d}, \tag{14}$$

ou seja,

$$r_{i+1} \equiv a_m u^{i+1} + a_{m-1} u^i + \cdots + a_{m-i} u + a_{m-i-1} \pmod{d}. \tag{15}$$

Logo, a afirmação vale para $i+1$ e, por indução, para todo $0 \leq i \leq m$. Em particular, para $i = m$,

$$r_m \equiv a_m u^m + a_{m-1} u^{m-1} + \cdots + a_0 = P(u) \pmod{d}. \tag{16}$$

Pelo Lema 2, $P(u) \equiv P(b) = N \pmod{d}$; portanto, $r_m \equiv N \pmod{d}$. ∎

Corolário 1. Nas condições da Proposição 1,

$$d \mid N \Leftrightarrow r_m \equiv 0 \pmod{d}. \tag{17}$$

Além disso, se r_m for reduzido ao conjunto $\{0,1,\ldots,d-1\}$, o valor obtido é o resto da divisão euclidiana de N por d.

Destaca-se a generalidade do resultado: a Proposição 1 vale para qualquer base $b \geq 2$ e qualquer divisor $d > 1$. Não é necessário supor $mdc(b,d)=1$ nem que b seja invertível módulo d.

4.2 UM EXEMPLO GENÉRICO

Antes dos exemplos numéricos, é instrutivo executar a recorrência com todos os dados arbitrários. Considere um número de quatro algarismos $N=(a_3a_2a_1a_0)_b$, uma base $b \geq 2$ e um divisor $d > 1$ quaisquer, e seja $u \equiv b \pmod{d}$. A recorrência de Horner produz, passo a passo:

$$r_0 = a_3, \tag{18}$$

$$r_1 \equiv r_0 u + a_2 = a_3 u + a_2 \pmod{d}, \tag{19}$$

$$r_2 \equiv r_1 u + a_1 \equiv a_3 u^2 + a_2 u + a_1 \pmod{d}, \tag{20}$$

$$r_3 \equiv r_2 u + a_0 \equiv a_3 u^3 + a_2 u^2 + a_1 u + a_0 = P(u) \equiv N \pmod{d}. \tag{21}$$

Cada etapa realiza uma única multiplicação por u, seguida da adição do algarismo seguinte; nenhuma potência de b é calculada explicitamente. O exemplo genérico também mostra como os critérios clássicos ficam contidos no esquema. Para $u=1$, a recorrência acumula a soma dos algarismos $a_3+a_2+a_1+a_0$. Para $u=-1$, os sinais se alternam a cada multiplicação e resulta $r_3 \equiv a_0 - a_1 + a_2 - a_3 \pmod{d}$. Para $u=0$ — o que ocorre quando $d \mid b$ —, cada etapa descarta o valor acumulado, pois $r_i \equiv r_{i-1} \cdot 0 + a_{m-i} = a_{m-i} \pmod{d}$, e resta apenas $r_3 \equiv a_0 \pmod{d}$: recupera-se o critério do último algarismo.

4.3 DOIS EXEMPLOS ESPECÍFICOS EM BASES DISTINTAS

Exemplo 1 (base 10, divisor 13). Considere $N=2925$ na base decimal e $d=13$. Como $10 \equiv -3 \pmod{13}$, toma-se $u=-3$. Os algarismos, do mais significativo ao menos significativo, são 2, 9, 2 e 5. Pela recorrência de Horner:

$$r_0 = 2, \tag{22}$$

$$r_1 \equiv 2 \cdot (-3) + 9 = 3 \pmod{13}, \tag{23}$$

$$r_2 \equiv 3 \cdot (-3) + 2 = -7 \pmod{13}, \tag{24}$$

$$r_3 \equiv (-7) \cdot (-3) + 5 = 26 \equiv 0 \pmod{13}. \tag{25}$$

Portanto, 2925 é divisível por 13 ; de fato, $2925 = 13 \cdot 225$. O valor intermediário -7 ilustra a diferença entre representante e resto: $-7 \equiv 6 \pmod{13}$, e 6 seria o valor obtido se cada etapa fosse reduzida ao intervalo $\{0, 1, \ldots, 12\}$. Ambas as escolhas conduzem à mesma conclusão.

Exemplo 2 (base 8, divisor 5). Considere agora o número octal $N = (2734)_8$, cujo valor decimal é

$$(2734)_8 = 2 \cdot 8^3 + 7 \cdot 8^2 + 3 \cdot 8 + 4 = 1500. \tag{26}$$

Como $8 \equiv 3 \pmod{5}$, toma-se $u = 3$ e aplica-se a mesma recorrência aos algarismos octais 2, 7, 3 e 4:

$$r_0 = 2, \tag{27}$$

$$r_1 \equiv 2 \cdot 3 + 7 = 13 \equiv 3 \pmod{5}, \tag{28}$$

$$r_2 \equiv 3 \cdot 3 + 3 = 12 \equiv 2 \pmod{5}, \tag{29}$$

$$r_3 \equiv 2 \cdot 3 + 4 = 10 \equiv 0 \pmod{5}. \tag{30}$$

Logo, $(2734)_8$ é divisível por 5; de fato, $1500 = 5 \cdot 300$. Observe que o procedimento operou apenas com os algarismos octais e com o resíduo $u = 3$; em nenhum momento foi necessário converter N para a base decimal.

Os dois exemplos executam exatamente a mesma recorrência; muda apenas o par (b, d) e, por consequência, o valor de u . Isso evidencia que o argumento da Seção 4.1 não depende de propriedades particulares da base decimal, mas somente da relação modular entre a base e o divisor.

4.4 CRITÉRIOS CLÁSSICOS COMO CASOS PARTICULARES

Os critérios clássicos surgem quando o resíduo da base possui forma especialmente simples. Três casos cobrem as regras mais conhecidas.

Caso 1: $b \equiv 1 \pmod{d}$. Tomando $u = 1$ no Lema 2, todas as potências $u^k = 1$ e

$$N \equiv a_m + a_{m-1} + \cdots + a_0 \pmod{d}. \tag{31}$$

O número é côngruo à soma dos seus algarismos. Na base decimal, isso explica os critérios de divisibilidade por 3 e por 9, pois $10 \equiv 1 (mod\, 3)$ e $10 \equiv 1 (mod\, 9)$. Por exemplo,

$$5832 = 5 \cdot 10^3 + 8 \cdot 10^2 + 3 \cdot 10 + 2. \tag{32}$$

Como $10 \equiv 1 (mod\, 9)$, tem-se

$$5832 \equiv 5 + 8 + 3 + 2 = 18 \equiv 0 (mod\, 9). \tag{33}$$

Logo, 5832 é divisível por 9; como $3 \mid 9$, conclui-se também que $3 \mid 5832$.

Caso 2: $b \equiv -1 (mod\, d)$. Tomando $u = -1$, tem-se $u^k = (-1)^k$, e os sinais dos termos se alternam:

$$N \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^m a_m (mod\, d). \tag{34}$$

Esse caso explica o critério de divisibilidade por 11 na base decimal, pois $10 \equiv -1 (mod\, 11)$. Para $N = 918082$, a soma alternada, a partir do algarismo das unidades, é

$$918082 \equiv 2 - 8 + 0 - 8 + 1 - 9 = -22 \equiv 0 (mod\, 11). \tag{35}$$

Logo, 918082 é divisível por 11; de fato, $918082 = 11 \cdot 83462$.

Caso 3: $b^k \equiv 0 (mod\, d)$ para algum $k \geq 1$, isto é, $d \mid b^k$. Para todo $j \geq k$, pode-se escrever $b^j = b^k \cdot b^{j-k}$; logo, $b^j \equiv 0 (mod\, d)$. Assim, na expansão

$$N = \sum_{j=0}^{m} a_j b^j, \tag{36}$$

todos os termos com $j \geq k$ se anulam módulo d, e resta apenas

$$N \equiv \sum_{j=0}^{k-1} a_j b^j (mod\, d). \tag{37}$$

A soma à direita é exatamente o número formado pelos k últimos algarismos de N na base b. Desse modo, quando $d \mid b^k$, a divisibilidade de N por d depende apenas desse bloco final. Na base decimal, isso explica os critérios que observam os últimos algarismos para divisores de potências de 10, como 2, 4, 8, 5, 25 e 125. Por exemplo, como

$$10^3 = 1000 \equiv 0 \pmod 8, \tag{38}$$

segue que $37248 \equiv 248 \pmod 8$. Como $248 = 31 \cdot 8$, conclui-se que 37248 é divisível por 8.

4.5 SOMA DE BLOCOS E ORDEM DA BASE

Suponha $mdc(b,d) = 1$. Nesse caso, está definida a ordem de b módulo d, denotada por $ord_d(b)$: o menor inteiro positivo q tal que $b^q \equiv 1 \pmod d$. Agrupando os algarismos de N, da direita para a esquerda, em blocos de q algarismos, obtêm-se inteiros $B_0, B_1, \ldots, B_s$, com $0 \le B_i < b^q$, tais que

$$N = B_s b^{qs} + B_{s-1} b^{q(s-1)} + \cdots + B_1 b^q + B_0. \tag{39}$$

Como $b^q \equiv 1 \pmod d$, todas as potências $b^{qi} \equiv 1 \pmod d$ e, portanto,

$$N \equiv B_s + B_{s-1} + \cdots + B_1 + B_0 \pmod d. \tag{40}$$

A soma dos blocos preserva o resto módulo d. Se $q = ord_d(b)$, esse é o menor tamanho de bloco possível para essa construção. Quando se usa outro expoente q' tal que $b^{q'} \equiv 1 \pmod d$ — necessariamente um múltiplo da ordem —, o critério continua válido, mas com blocos maiores que o necessário.

Esse é o fundamento dos critérios por blocos apresentados por Pereira e Ribas (2025) para a base decimal. Pela ótica deste artigo, trata-se da Proposição 1 aplicada à base agrupada b^q: quando $b^q \equiv 1 \pmod d$, a recorrência aninhada se reduz a uma soma de blocos.

Exemplo. Como

$$10^3 = 1000 \equiv 1 \pmod{37}, \tag{41}$$

pode-se testar a divisibilidade por 37, na base decimal, somando blocos de três algarismos. Para $N = 123321$, tem-se

$$123321 = 123 \cdot 1000 + 321 \equiv 123 + 321 = 444 \pmod{37}. \tag{42}$$

Como $444 = 12 \cdot 37$, conclui-se que 123321 é divisível por 37.

4.6 CRITÉRIOS QUE PRESERVAM O RESTO E CRITÉRIOS POR UNIDADES MODULARES

Uma transformação T preserva o resto módulo d quando

$$T(N) \equiv N \pmod{d}. \tag{43}$$

Nesse caso, $T(N)$ e N pertencem à mesma classe de congruência; se ambos forem reduzidos ao conjunto $\{0,1,\ldots,d-1\}$, terão o mesmo resto na divisão por d. A recorrência de Horner possui essa propriedade, pois constrói um valor congruente ao número original (Proposição 1).

Outra classe de critérios preserva apenas a divisibilidade. Isso ocorre, por exemplo, quando existe uma unidade c módulo d — isto é, um inteiro c invertível em Z/dZ — tal que

$$T(N) \equiv cN \pmod{d}. \tag{44}$$

Como c é invertível módulo d,

$$T(N) \equiv 0 \pmod{d} \Leftrightarrow N \equiv 0 \pmod{d}. \tag{45}$$

Assim, T decide corretamente a divisibilidade por d, mas não preserva, em geral, o resto original.

Um caso importante aparece quando se escreve

$$N = bx + y, \tag{46}$$

em que y é o último algarismo de N na base b e x é o número formado pelos demais algarismos. Se $mdc(b,d)=1$, existe λ tal que $\lambda b \equiv 1 \pmod{d}$. Multiplicando N por λ, obtém-se

$$\lambda N = \lambda bx + \lambda y \equiv x + \lambda y \pmod{d}. \tag{47}$$

Logo,

$$d \mid N \Leftrightarrow d \mid (x + \lambda y). \tag{48}$$

Esse critério é válido para decidir a divisibilidade, mas calcula uma quantidade congruente a λN, não necessariamente a N. Portanto, em geral, não preserva o resto.

Na base decimal, para $d=7$, o inverso de 10 é 5, pois $10 \cdot 5 = 50 \equiv 1 \pmod{7}$; além disso, $5 \equiv -2 \pmod{7}$. Assim, se $N = 10x + y$, então

$$5N \equiv x - 2y \pmod{7}. \tag{49}$$

Como 5 é invertível módulo 7,

$$7 \mid N \Leftrightarrow 7 \mid (x-2y). \tag{50}$$

Por exemplo, $203=10\cdot 20+3$. Aplicando o critério, $20-2\cdot 3=14$. Como 14 é divisível por 7, conclui-se que 203 é divisível por 7; de fato, $203=7\cdot 29$.

O resto, porém, não é preservado em geral. Para $N=123$, tem-se $123\equiv 4\,(mod\,7)$, mas

$$T(123)=12-2\cdot 3=6, e\, 6\not\equiv\ 4\,(mod\,7). \tag{51}$$

A divisibilidade é preservada; o resto, não.

O mesmo procedimento pode ser aplicado em outras bases. Para $d=7$, alguns casos são apresentados na Tabela 1.

Tabela 1. Critérios do tipo x + λy para o divisor 7 em bases distintas

Base b	b (mod 7)	$\lambda = b^{-1}$ (mod 7)	Critério para N = bx + y
8	1	1	$x+y$
10	3	$5\equiv -2$	$x-2y$
12	5	3	$x+3y$
16	2	$4\equiv -3$	$x-3y$

Fonte: Elaborado pelos autores, 2026

Em base 12, por exemplo, $12^{-1}\equiv 3\,(mod\,7)$, pois $12\cdot 3=36\equiv 1\,(mod\,7)$. Logo, para $N=12x+y$, o critério correspondente é $x+3y$. Tomando

$$(41)_{12}=12\cdot 4+1=49, \tag{52}$$

obtém-se $4+3\cdot 1=7$. Portanto, $(41)_{12}$ é divisível por 7; de fato, $49=7\cdot 7$.

4.7 CRITÉRIOS CLÁSSICOS EM OUTRAS BASES

Os casos da Seção 4.4 também não dependem da base decimal. Em base 12, tem-se $12\equiv 1\,(mod\,11)$; logo, um número escrito em base 12 é divisível por 11 quando a soma de seus algarismos é divisível por 11. Por exemplo, usando $B=11$ como algarismo,

$$(2B9)_{12}=2\cdot 12^2+11\cdot 12+9=429. \tag{53}$$

A soma dos algarismos é $2+11+9=22$, que é divisível por 11. Portanto, $(2B9)_{12}$ é divisível por 11; de fato, $429=11\cdot 39$.

Em base 8, tem-se $8 \equiv -1 \pmod 9$. Para $(121)_8$, a soma alternada, a partir do algarismo das unidades, é $1-2+1=0$; logo, $(121)_8$ é divisível por 9. De fato,

$$(121)_8 = 1 \cdot 8^2 + 2 \cdot 8 + 1 = 81 = 9 \cdot 9. \tag{54}$$

Em base 16, tem-se $16 \equiv 1 \pmod{15}$. Usando $A=10$ como algarismo, para $(2\,A\,3)_{16}$ a soma dos algarismos é $2+10+3=15$; logo, o número é divisível por 15. De fato,

$$(2\,A\,3)_{16} = 2 \cdot 16^2 + 10 \cdot 16 + 3 = 675 = 45 \cdot 15. \tag{55}$$

Esses exemplos confirmam que a estrutura dos critérios depende apenas da relação modular entre a base e o divisor, e não de propriedades particulares da base decimal.

4.8 SÍNTESE DAS CLASSES DE CRITÉRIOS

A Tabela 2 resume as situações discutidas.

Tabela 2. Classes de critérios de divisibilidade segundo a condição modular

Condição modular	Critério obtido	Preserva o resto?	Exemplo
$b \equiv 1 \pmod d$	Soma dos algarismos	Sim	3 e 9 na base 10
$b \equiv -1 \pmod d$	Soma alternada	Sim	11 na base 10
$b^k \equiv 0 \pmod d$	Últimos k algarismos	Sim	8, 16 e 25 na base 10
$b^q \equiv 1 \pmod d$	Soma de blocos	Sim	37 na base 10
$T(N) \equiv cN \pmod d$, com c unidade	Critério equivalente de divisibilidade	Não necessariamente	Critério do 7: $x-2y$

Fonte: Elaborado pelos autores, 2026

A classificação separa os critérios que calculam a mesma classe de congruência do número original daqueles que apenas preservam a resposta à pergunta “é divisível por d ?”. Essa diferença é matemática, não apenas terminológica: no primeiro grupo, o procedimento fornece o resto; no segundo, somente a decisão de divisibilidade.

5 CONSIDERAÇÕES FINAIS

Conclui-se que critérios de divisibilidade podem ser descritos como avaliações modulares da representação posicional. Dado um número escrito na base b , sua expansão define um polinômio dos dígitos; ao reduzir b módulo d , obtém-se uma forma equivalente de calcular a classe de congruência do número módulo d .

A recorrência de Horner fornece o procedimento geral para essa avaliação: percorre os algarismos uma única vez e produz um representante congruente ao número original. Quando esse representante é reduzido ao conjunto $\{0,1,\ldots,d-1\}$, obtém-se o resto da divisão por d. A exposição em três níveis — forma geral, exemplo genérico e exemplos em bases distintas — evidencia que o argumento depende apenas da relação modular entre a base e o divisor.

Os critérios clássicos aparecem quando a base, ou uma potência da base, assume resíduos simples módulo o divisor: a soma dos algarismos decorre de $b \equiv 1 (mod\, d)$; a soma alternada, de $b \equiv -1 (mod\, d)$; os critérios pelos últimos algarismos, de $b^k \equiv 0 (mod\, d)$; e a soma de blocos, de $b^q \equiv 1 (mod\, d)$.

A distinção entre critérios que preservam o resto e critérios que preservam apenas a divisibilidade evita tratar regras diferentes como se conservassem a mesma informação. O trabalho não apresenta um critério universal inédito nem prova minimalidade computacional. Sua contribuição é organizar os critérios em uma estrutura comum, com hipóteses explícitas e demonstrações por congruência modular.

REFERÊNCIAS

ALEXEEV, Boris. Minimal DFAs for testing divisibility. **Journal of Computer and System Sciences**, v. 69, n. 2, p. 235-243, 2004. DOI: 10.1016/j.jcss.2004.02.001. Disponível em: https://www.sciencedirect.com/science/article/pii/S0022000004000200. Acesso em: 7 jul. 2026.

GRINBERG, Anatoly A.; LURYI, Serge. **General Divisibility Criteria**. arXiv, 2014. DOI: 10.48550/arXiv.1401.5486. Disponível em: https://arxiv.org/abs/1401.5486. Acesso em: 7 jul. 2026.

HORNER, William George. XXI. A new method of solving numerical equations of all orders, by continuous approximation. **Philosophical Transactions of the Royal Society of London**, v. 109, p. 308-335, 1819. DOI: 10.1098/rstl.1819.0023. Disponível em: https://doi.org/10.1098/rstl.1819.0023. Acesso em: 7 jul. 2026.

KNUTH, Donald E. **The Art of Computer Programming**. Volume 2: Seminumerical Algorithms. 3. ed. Boston: Addison-Wesley, 1997.

MARTINEZ, Fabio; MOREIRA, Carlos; SALDANHA, Nicolau; TENGAN, Eduardo. **Teoria dos números**: um passeio com primos e outros números familiares pelo mundo inteiro. 5. ed. Rio de Janeiro: IMPA, 2018.

PEREIRA, Athos de Azevedo; RIBAS, Sávio. Critérios de Divisibilidade. **Revista de Matemática da UFOP**, v. 1, n. 1, 2025. DOI: 10.63801/rmat.v1i.7879. Disponível em: https://periodicos.ufop.br/rmat/article/view/7879. Acesso em: 7 jul. 2026.

SUTNER, Klaus. Divisibility and State Complexity. **The Mathematica Journal**, v. 11, n. 3, p. 430-445, 2010. DOI: 10.3888/tmj.11.3-8. Disponível em: https://www.mathematica-journal.com/2010/02/05/divisibility-and-state-complexity/. Acesso em: 7 jul. 2026.