RMAT
ISSN: 2237-8103
REVISTA DE MATEMÁTICA DA UFOP

OPEN ACCESS
Volume 1, Número 1, 2025
10.63801/rmat.v1i.7879
Recebido: 22/02/2025
Publicado: 08/10/2025

# Critérios de Divisibilidade

*Divisibility Criteria*
*Criterios de divisibilidad*

**Athos de Azevedo Pereira**
<athos.pereira@aluno.ufop.edu.br>
Universidade Federal de Ouro Preto, Ouro Preto, MG, Brasil
<https://orcid.org/0009-0002-9044-4918>
<https://lattes.cnpq.br/1676243889230050>

**Sávio Ribas**
<savio.ribas@ufop.edu.br>
Universidade Federal de Ouro Preto, Ouro Preto, MG, Brasil
<https://orcid.org/0000-0002-8632-4764>

**Resumo**
*Neste trabalho, veremos como construir, para números escritos na base decimal, critérios de divisibilidade por um inteiro qualquer $d > 1$. Para isso, usaremos congruências e a ordem de $10$ módulo $d$ para explicar a construção desses critérios. Exibiremos alguns critérios que serão úteis e outros nem tanto, mas que podem ser aplicados computacionalmente. Tais critérios englobam os casos conhecidos de divisibilidade por $2$, $4$, $8$, $5$, $25$, $3$, $9$ e $11$, além de outros pouco conhecidos, porém simples, como é o caso do $37$. Além disso, se $d$ é uma potência de primo, então os critérios apresentados, quando não houver divisibilidade por $d$, irão preservar o resto.*

***Palavras-chave:*** *Critérios de divisibilidade. Congruência. Ordem.*

**Abstract**
*In this paper, we will explore how to construct divisibility criteria for numbers written in the decimal base by any integer $d > 1$. To achieve this, we will use congruences and the order of $10$ modulo $d$ to explain the construction of these criteria. We will present some criteria that are useful and others that may not be as practical but can still be applied computationally. These criteria include the well-known cases of divisibility by $2$, $4$, $8$, $5$, $25$, $3$, $9$, and $11$, as well as lesser-known yet simple cases, such as $37$. Furthermore, if $d$ is a prime power, the presented criteria will preserve the remainder when divisibility by $d$ does not hold.*

***Keywords:*** *Divisibility criteria. Congruence. Order*

**Resumen**
*En este artículo veremos cómo construir criterios de divisibilidad para cualquier número entero $d > 1$ para números escritos en base decimal. Para ello, utilizaremos las congruencias y el orden de $10$ módulo $d$ para explicar la construcción de estos criterios. Mostraremos algunos criterios que serán útiles y otros que no lo son tanto, pero que pueden aplicarse computacionalmente. Estos criterios incluyen los conocidos casos de divisibilidad por $2$, $4$, $8$, $5$, $25$, $3$, $9$ y $11$, así como otros poco conocidos pero sencillos, como $37$. Además, si $d$ es una potencia de primo, entonces los criterios presentados, cuando no hay divisibilidad por $d$, preservarán el resto.*

***Palabras-Clave:*** *Criterios de divisibilidad. Congruencia. Orden.*

## 1. INTRODUÇÃO

Ainda nos primeiros anos da educação básica, os critérios de divisibilidade por certos números, como $2, 3, 4, 5, 6, 8, 9, 10$ e $11$ são apresentados para os estudantes como uma maneira mais eficiente de realizar divisões por estes números. Entretanto, com frequêcia, estes critérios carecem de justificativas, sendo mostrados por meio de exemplos de aplicação. Neste artigo, contruíremos, na base decimal, os critérios de divisibilidade para qualquer inteiro $d > 1$.

Inicialmente vamos apresentar algumas definições, teoremas e propriedades que nos auxiliarão na construção dos critérios de divisibilidade; em especial, utilizaremos os conceitos de congruências e ordem. Dentre os critérios que apresentaremos neste artigo estão a divisibilidade por potências de $2$ e de $5$, divisibilidade por $3, 9$ e $11$ e o caso geral de divisibilidade por qualquer inteiro $d > 1$. Também mostraremos critérios que são pouco práticos para serem usados no cotidiano, mas que podem ser aplicados de outras formas.

Por fim, comentaremos sobre os critérios que não preservam o resto quando não há divisibilidade por $d$. Dizemos que um critério de divisibilidade por um inteiro $d > 1$ *preserva resto* quando, para todo inteiro positivo $n$, ao aplicar o critério, o resto da divisão da saída do algoritmo na divisão por $d$ é o mesmo resto da divisão de $n$ por $d$. Se esse resto for $0$, ambos são divisíveis por $d$. Na literatura, geralmente os critérios de divisibilidade são enunciados levando-se em consideração apenas quando $n$ é divisível por $d$.

O artigo está organizado da seguinte forma. Na Seção 2, apresentamos, com demonstração, todos os resultados preliminares que usaremos ao longo das seções seguintes. Na Seção 3, apresentamos os critérios de divisibilidade. Em um primeiro momento, apresentamos de forma geral os critérios que preservam o resto, assim como uma proposição que trata da multiplicatividade dos critérios. Em seguida, apresentamos os critérios que não necessariamente preservam o resto, mas que acabam por serem mais simplificados que os que preservam. Finalmente, toda a discussão é sintetizada na Seção 4.

## 2. PRELIMINARES

Vamos apresentar nessa seção as definições, proposições, teoremas e propriedades que usaremos nesse artigo. Começaremos pelas definições de divisibilidade e máximo divisor comum, passaremos também pelo Teorema de Bézout e pelo Teorema Fundamental da Aritmética. Finalmente veremos sobre congruência, bases, função $\varphi$ de Euler, Teorema de Euler e ordem, que serão tópicos cruciais para obtermos os critérios de divisibilidade.

### 2.1. Divisibilidade

**Definiçao 1.** *Dados $a, d$ inteiros, dizemos que $d$* divide *$a$ (ou $d$ é um* divisor *de $a$ ou ainda $a$ é* múltiplo *de $d$) e escrevemos $d \mid a$ se existe um $q$ inteiro tal que $a = qd$. Senão, escrevemos $d \nmid a$.*

**Exemplo 2.** *Temos que $5 \mid 10$, porém $10 \nmid 5$.*

Vamos ver agora algumas propriedades importantes divisibilidade:

**Lema 3.** *Sejam $a, b, c \in \mathbb{Z}$. Temos*

1. *Se $a \mid b$ e $b \mid c$, então $a \mid c$.*
2. *$a \mid b$ se, e somente se $a \mid (b + ca)$.*

*Demonstração.* 1. Se $a \mid b$ e $b \mid c$, existem $k_1$ e $k_2 \in \mathbb{Z}$ tais que $b = ak_1$ e $c = bk_2$, temos então que $c = ak_1k_2$, logo $a \mid c$.

2. $(\Rightarrow)$ Se $a \mid b$, existe $k_1 \in \mathbb{Z}$ tal que $b = ak_1$. Como $a \mid a$, segue-se que $a \mid a(k_1 + c)$, logo $a \mid b + c$.
   $(\Leftarrow)$ Se $a \mid (b + ca)$, existe $k_2 \in \mathbb{Z}$ tal que $(b + ca) = ak_2 \Leftrightarrow b = a(k_2 - c)$. Portanto $a \mid b$.
   Assim, $a \mid b \Leftrightarrow a \mid (b + ca)$, como queriamos demonstrar. □

### 2.2. Máximo Divisor Comum

**Definiçao 4.** *Definimos o* máximo divisor comum *entre dois inteiros $a$ e $b$, $\mathrm{mdc}(a, b)$, como o maior inteiro positivo que divide $a$ e $b$ ao mesmo tempo. Por convenção, $\mathrm{mdc}(0, 0) = 0$.*

**Exemplo 5.** *Os divisores positivos de $12$ são $1, 2, 3, 4, 6, 12$. Os divisores positivos de $18$ são $1, 2, 3, 6, 9, 18$. O maior inteiro que divide $12$ e $18$ ao mesmo tempo é $6$, logo $\mathrm{mdc}(12, 18) = 6$.*

O próximo teorema diz que o $\mathrm{mdc}(a, b)$ de dois inteiros $a$ e $b$ pode ser escrito como a combinação linear entre $a$ e $b$.

**Teorema 6** (Bézout). *Sejam $a, b \in \mathbb{Z}$. Então existem $x, y \in \mathbb{Z}$ com $ax + by = \mathrm{mdc}(a, b)$. Em particular, se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$ então $c \mid \mathrm{mdc}(a, b)$.*

*Demonstração.* Considere o conjunto $A$, formado pelas combinações lineares de $a$ e $b$:

$$A = \{ax + by; x, y \in \mathbb{Z}\}.$$

Como $A$ possui elementos positivos, podemos considerar $A \cap \mathbb{N}$, que é não vazia. Segue do Princípio da Boa Ordem que a interseção $A \cap \mathbb{N}$ tem elemento mínimo. Seja $d = ax_0 + by_0$ o elemento mínimo de $A$. Vamos verificar que $d$ divide $a$ e $b$ simultaneamente. Suponha por contradição que $d \nmid a$. Temos que existem $q$ e $r$ inteiros tais que $a = qd + r$ com $0 < r < d$. Daí obtemos $r = a - qd = a - q(ax_0 + by_0) = a(1 - qx_0) - qby_0$. Logo, $r \in A$ e $r < d$, o que é uma contradição, pois $d$ é o elemento mínimo do conjunto $A$. Portanto $d \mid a$. Analogamente verificamos que $d \mid b$. Seja $c = \mathrm{mdc}(a, b)$. Como $c \mid a$ e $c \mid b$ existem inteiros $k_1$ e $k_2$ tais que $a = k_1c$ e $b = k_2c$. Daí, $d = ax_0 + by_0 = x_0k_1c + y_0k_2c = c(x_0k_1 + y_0k_2)$, ou seja, $d \mid c$. Logo $c \geq d$, e como $d = \mathrm{mdc}(a, b)$, segue-se$d \geq c$. Portanto, $c = d = ax_0 + by_0$. □

**Definiçao 7.** *Um número inteiro $n \geq 2$ é primo se seus únicos divisores positivos são $1$ e $n$. Caso contrário, $n$ é dito composto.*

Do Teorema de Bézout seguem as seguintes propriedades:

1. Se $\mathrm{mdc}(a, b) = 1$ e $a \mid bc$, então $a \mid c$. De fato, existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$, portanto $acx + bcy = c$. Como $a$ divide o lado esquerdo, devemos ter $a \mid c$.
2. Se $p$ é primo, $a_1, \ldots, a_n \in \mathbb{Z}$ e $p \mid (a_1 \ldots a_n)$, então $p \mid a_i$ para algum $i \in \{1, \ldots, n\}$. Isso ocorre pois se $p \nmid a_j$, então $\mathrm{mdc}(p, a_j) = 1$, e assim podemos aplicar o item anterior.

### 2.3. Teorema Fundamental da Aritmética

**Teorema 8** (Teorema Fundamental da Aritmética). *Seja $n \geq 2$ um inteiro. Então $n$ pode ser escrito de forma única (a menos da ordem dos fatores) como produto de primos, isto é, $n = p_1 \cdots p_m$, em que $m$ é um inteiro positivo e $p_1 \leq \cdots \leq p_m$ são primos.*

*Demonstração.* Vamos demonstrar a existência por indução forte.
Base: $n = 2$ é primo (pode ser escrito como $n = p_1$, onde $p_1 = 2$).
Hipótese: Suponha que todo inteiro $k$ tal que $2 \leq k \leq n$ possa ser escrito como produto de primos.
Passo indutivo: Se $n + 1$ é primo, não há o que fazer. Se $n + 1$ é composto, é possível escrever $n + 1 = ab$, $2 \leq a, b \leq n$. Por hipótese, $a$ e $b$ podem ser decompostos como produto de primos. Juntando e reordenando as os fatores de $a$ e $b$ obtemos uma fatoração de $n + 1$.

Vamos agora provar a unicidade. Suponha que $n$ possa ser escrito como produto de primos de duas formas distintas, isto é, $n = p_1 \cdots p_r$ e $n = q_1 \cdots q_s$. Temos $p_1 \ldots p_r = q_1 \ldots q_s$. Daí segue-se $p_1 \mid q_1 \ldots q_s$. Como $p_1$ é primo, obtemos $p_1 = q_j$ para algum $1 \leq j \leq s$. Suponhamos sem perda de generalidade que $j = 1$, isto é, $p_1 = q_1$. Então $p_2 \ldots p_r = q_2 \ldots q_s$ e, indutivamente e sem perda de generalidade, obtemos $p_i = q_i$ para todo $i$. Notemos que isso implica que $r = s$ e a fatoração é única a menos da ordem dos fatores. □

### 2.4. Congruências

**Definiçao 9.** *Sejam $a, b, n$ inteiros com $n \geq 2$. Dizemos que $a$ é* congruente *a $b$ módulo $n$ e escrevemos $a \equiv b \pmod{n}$ se $n \mid a - b$. Isso é equivalente a $a$ e $b$ deixarem o mesmo resto na divisão por $n$.*

**Exemplo 10.** $19 \equiv 11 \pmod{2}$, *já que* $2 \mid 19 - 11$. *Perceba que* $19$ *e* $11$ *deixam resto igual a* $1$ *na divisão por* $2$.

**Proposição 11.** *Para quaisquer $a, b, c, d, n \in \mathbb{Z}$ com $n \geq 2$, são válidos:*

1. $a \equiv a \pmod{n}$.
2. *Se* $a \equiv b \pmod{n}$, *então* $b \equiv a \pmod{n}$.
3. *Se* $a \equiv b \pmod{n}$ *e* $b \equiv c \pmod{n}$, *então* $a \equiv c \pmod{n}$.
4. *Se* $a \equiv b \pmod{n}$ *e* $c \equiv d \pmod{n}$, *então* $a \pm c \equiv b \pm d \pmod{n}$. *Particularmente, se* $a \equiv b \pmod{n}$, *então* $ak \equiv bk \pmod{n}$ *para todo* $k \in \mathbb{Z}$.
5. *Se* $a \equiv b \pmod{n}$ *e* $c \equiv d \pmod{n}$, *então* $ac \equiv bd \pmod{n}$. *Em particular, se* $a \equiv b \pmod{n}$, *então* $a^k \equiv b^k \pmod{n}$ *para todo* $k \in \mathbb{N}$.
6. *Se* $ac \equiv bc \pmod{n}$, *então* $a \equiv b \pmod{\frac{n}{\mathrm{mdc}(c,n)}}$. *Em particular, se* $\mathrm{mdc}(c, n) = 1$, *então* $ac \equiv bc \pmod{n}$ *se, e somente se* $a \equiv b \pmod{n}$.

*Demonstração.* 1. Temos que $n \mid 0$, daí $n \mid a - a$ e então $a \equiv a \pmod{n}$.

2. Se $a \equiv b \pmod{n}$, então existe um inteiro $k_1$ tal que $a = k_1 n + b$, daí $b = -k_1 n + a$, isto é, $b \equiv a \pmod{n}$.

3. Se $a \equiv b$ e $b \equiv c$, existem $k_1$ e $k_2 \in \mathbb{Z}$ tais que $a = k_1 n + b$ e $b = k_2 n + c$. Daí segue-se $a = (k_1 + k_2)n + c$, ou seja $a \equiv c \pmod{n}$.

4. Se $a \equiv b$ e $c \equiv d$, existem $k_1$ e $k_2 \in \mathbb{Z}$ tais que $a - b = k_1 n$ e $c - d = k_2 n$. Somando as equações obtemos $a - b + (c - d) = k_1 n + k_2 n \Leftrightarrow a + c - (b + d) = n(k_1 + k_2)$, isto é, $a + c \equiv b + d \pmod{n}$. A prova para subtração é análoga.

5. Se $a \equiv b$ e $c \equiv d$, existem $k_1$ e $k_2 \in \mathbb{Z}$ tais que $a - b = k_1 n$ e $c - d = k_2 n$, portanto $ac - bc = ck_1 n$ e $cb - db = bk_2 n$. Somando as novas equações encontradas obtemos $ac - bd = n(ck_1 + bk_2)$, isto é, $ac \equiv bd \pmod{n}$.

6. Seja $d = \mathrm{mdc}(c, n)$. Da hipótese, temos que $n \mid c(a - b)$. Dividindo ambos os lados por $d$, segue-se $\frac{n}{d} \mid \frac{c}{d}(a - b)$. Como $\mathrm{mdc}\left(\frac{c}{d}, \frac{n}{d}\right) = 1$, devemos ter $\frac{n}{d} \mid (a - b)$, o que implica que $a \equiv b \pmod{\frac{n}{d}}$.

□

**Definiçao 12.** *Sejam $a, b, n$ inteiros com $n \geq 2$. Dizemos que $a$ é* invertível módulo $n$ quando existe $b$ tal que $ab \equiv 1 \pmod{n}$. Chamamos $b$ de *inverso (multiplicativo) de $a$ módulo $n$.*

O próximo resultado exibe a condição de existência do inverso de $a$ módulo $n$.

**Proposição 13.** *Sejam $a, n$ inteiros com $n \geq 2$. Então $a$ é invertível módulo $n$ se e somente se $\mathrm{mdc}(a, n) = 1$.*

*Demonstração.* A congruência $ab \equiv 1 \pmod{n}$ tem solução na variável $b$ se, e só se, existem $b$ e $k$ inteiros tais que $ab - 1 = nk \Leftrightarrow ab - nk = 1$. Pelo Teorema 6, a equação admite solução inteira se, e somente se, $\mathrm{mdc}(a, n) = 1$. □

### 2.5. Bases

**Teorema 14.** *Seja $d \geq 2$ um inteiro. Então qualquer inteiro $n \geq 0$ pode ser representado de forma única como*

$$n = a_k d^k + a_{k-1} d^{k-1} + \cdots + a_2 d^2 + a_1 d^1 + a_0,$$

*onde $a_k \neq 0$, $0 \leq a_j < d$ e $a_j \in \mathbb{Z}$ para todo $0 \leq j \leq k$. Dizemos que $n$ escrito dessa forma está na* base *$d$ e os números $a_0, \ldots, a_k$ são os* dígitos *(ou* algarismos*) de $n$ na base $d$.*

**Notação.** $n = (a_k a_{k-1} a_{k-2} \cdots a_2 a_1 a_0)_d$.
*Por comodidade, na base decimal (isto é, para $d = 10$) omitimos os parênteses e não explicitamos a base: $(n)_{10} = n$.*

*Demonstração.* Vamos provar a existência por indução.
Base: Para $n = 1$, temos que $a_0 = 1$ e $k = 0$. O teorema é verdade para $n = 1$.
Hipótese: Suponha que para todo inteiro menor que $n$ o teorema seja verdadeiro.
Passo indutivo: Como $d > 1$ e $n > 0$, $n$ está entre dois dos números da sequências $d^0, d^1, \cdots,$

$d^i, \cdots$. Então, existe um inteiro $k$ tal que $d^k \leq n < d^{k+1}$. Daí, $n = a_k d^k + r$ com $0 < a \leq d$ e $0 \leq r < d^k$. Se $r = 0$, então $n = a_k d^k + 0 + \cdots + 0 + 0$. Se $r \neq 0$, então por hipótese $r$ pode ser escrito como $r = b_j d^j + b_{j-1} d^{j-1} + \cdots + b_2 d^2 + b_1 d^1 + b_0$ para algum $j \leq k-1$. Portanto, $n = a_k d^k + b_j d^j + b_{j-1} d^{j-1} + \cdots + b_2 j^2 + b_1 d^1 + b_0$.

Vamos provar a unicidade do teorema. Suponha que existam duas representações distintas para um número $n$ na mesma base $d$, digamos $n = a_k d^k + \cdots + a_0$ e $n = b_k d^k + \cdots + b_0$. Como as representações são diferentes, existe um menor índice $j$ tal que $a_j \neq b_j$. É possível escrever $a_j + a_{j+1} d + \ldots a_k d^{k-j} = b_j + b_{j+1} d + \cdots + b_k d^{k-j}$, daí $a_j \equiv b_j \pmod{d}$, o que é absurdo, pois $0 < |a_j - b_j| < d$. Logo, $a_j - b_j$ não pode ser múltiplo de $d$. Portanto a representação é única. □

**Exemplo 15.** *O número* $35564$, *que está escrito na base* $10$, *é escrito na base* $7$ *como* $(205454)_7$, *pois* $(205454)_7 = 2 \cdot 7^5 + 0 \cdot 7^4 + 5 \cdot 7^3 + 4 \cdot 7^2 + 5 \cdot 7^1 + 4 \cdot 7^0 = 35564$.

### 2.6. A Função $\varphi$ de Euler

Se $A$ é um conjunto qualquer, então $\#A$ denota a cardinalidade de $A$.

**Definiçao 16.** *A função* $\varphi$ *de Euler*

$$\varphi(n) = \#\{1 \leq a \leq n;\ \mathrm{mdc}(a, n) = 1\}$$

*representa o número de inteiros positivos menores ou iguais a* $n$ *que são coprimos com* $n$.

**Exemplo 17.** *Vamos calcular* $\varphi(10)$ *e* $\varphi(11)$. *Temos que*

$$\varphi(10) = \#\{1 \leq a \leq 10;\ \mathrm{mdc}(a, 10) = 1\} = \#\{1, 3, 7, 9\} = 4,$$
$$\varphi(11) = \#\{1 \leq a \leq 11;\ \mathrm{mdc}(a, 11) = 1\} = \#\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} = 10.$$

**Teorema 18** (Euler). *Se* $a, n$ *são inteiros coprimos com* $n \geq 2$, *então* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

*Demonstração.* A demonstração pode ser encontrada em (MARTINEZ *et al.*, 2018, Teorema 1.40). □

### 2.7. Ordem

**Definiçao 19.** *Sejam* $n \geq 2$ *um inteiro e* $a$ *um inteiro coprimo com* $n$. A ordem de $a$ módulo $n$ *é o menor inteiro* $t > 0$ *tal que* $a^t \equiv 1 \pmod{n}$.

**Notação.** $t = \mathrm{ord}_n a$.

Dados $n \geq 2$ e $a$ coprimo com $n$, a ordem $\mathrm{ord}_n a$ existe pois sendo $1, a, a^2, a^3, \ldots$ uma sequência infinita, pelo Princípio da Casa dos Pombos existem $i > j$ inteiros não-negativos tais que $a^i \equiv a^j \pmod{n}$. Como $\mathrm{mdc}(a, n) = 1$, multiplicamos a congruência anterior por $a^{-j}$ e obtemos $a^{i-j} \equiv 1 \pmod{n}$.

Usando o Teorema 18, segue-se $\mathrm{ord}_n a \leq \varphi(n)$.

**Exemplo 20.** *Vamos calcular a ordem de* $10$ *módulo* $7$*:*

$$\begin{aligned} 10^1 &\equiv 3 \pmod 7 & 10^4 &\equiv 4 \pmod 7 \\ 10^2 &\equiv 2 \pmod 7 & 10^5 &\equiv 5 \pmod 7 \\ 10^3 &\equiv 6 \pmod 7 & 10^6 &\equiv 1 \pmod 7, \end{aligned}$$

*ou seja,* $\mathrm{ord}_7 10 = 6$*, pois* $j = 6$ *é o menor inteiro positivo* $j$ *tal que* $10^j \equiv 1 \pmod 7$.

**Proposição 21.** *Sejam* $a$ *e* $n$ *inteiros coprimos com* $n \geq 2$*. Temos que* $a^t \equiv 1 \pmod n$ *se, e somente se,* $\mathrm{ord}_n a \mid t$.

*Demonstração.* ($\Rightarrow$) Se $a^t \equiv 1 \pmod n$, existem inteiros $q$ e $r$ com $0 \leq r \leq \mathrm{ord}_n a$ tal que $t = (\mathrm{ord}_n a)q + r$. Daí, $1 \equiv a^{(\mathrm{ord}_n a)q + r} = a^{(\mathrm{ord}_n a)q} a^r \equiv a^r \pmod n$. Pela minimalidade da ordem, devemos ter que $r = 0$, isto é, $\mathrm{ord}_n a \mid t$.
($\Leftarrow$) Se $\mathrm{ord}_n a \mid t$, existe um inteiro positivo $k$ tal que $t = k\mathrm{ord}_n a$. Assim, $a^t \equiv a^{(\mathrm{ord}_n a)k} \pmod n$, ou seja $a^t \equiv 1 \pmod n$. □

**Corolário 22.** *Sejam* $a$ *e* $n$ *inteiros coprimos com* $n \geq 2$*. Então,* $\mathrm{ord}_n a \mid \varphi(n)$.

*Demonstração.* Tome $t = \varphi(n)$ na proposição anterior. □

## 3. CRITÉRIOS DE DIVISIBILIDADE

Nessa seção, apresentamos a construção dos critérios de divisibilidade. Começamos pela divisibilidade por potências de $2$ e $5$. Na sequência, veremos os critérios por $3$, $9$ e $11$ e o caso geral de divisibilidade, finalizando com os critérios por $7$, $13$ e $37$ que preservam resto, além de um critério mais simples por $7$ que não preserva resto.

### 3.1. Divisibilidade por potências de $2$ e por potências de $5$

**Proposição 23.** *Um número deixa o mesmo resto na divisão por* $2^k$*,* $k$ *inteiro com* $k \geq 1$*, que o número formado pelos seus* $k$ *últimos algarismos.*

*Demonstração.* Seja $n \geq 0$ um inteiro escrito na base $10$ como $n = a_r a_{r-1} \ldots a_1 a_0$. Como $2^k \mid 10^k$, segue-se $10^j \equiv 0 \pmod{2^k}$ para todo $j \geq k$. Logo,

$$\begin{aligned} n &= a_r 10^r + \cdots + a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \\ &\equiv 0 + \cdots + 0 + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \\ &\equiv (a_{k-1} \ldots a_0)_{10} \pmod{2^k}, \end{aligned}$$

como queríamos. □

Como consequência da proposição anterior, seguem os conhecidos critérios de divisibilidade por $2$ e $4$:

- Um número deixa o mesmo resto na divisão por $2$ que o seu último algarismo.

- Um número deixa o mesmo resto na divisão por $4$ que o número formado pelo seus dois últimos algarismos.

Como $5^k \mid 10^k$, um argumento completamente análogo mostra o seguinte critério de divisibilidade por potências de $5$.

**Proposição 24.** *Um número deixa o mesmo resto na divisão por $5^k$, $k$ inteiro com $k \geq 1$, que o número formado pelos seus $k$ últimos algarismos.*

Como resultado da proposição, seguem os seguintes critérios de divisibilidade por $5$ e $25$.

- Um número deixa o mesmo resto na divisão por $5$ que o seu último algarismo.
- Um número deixa o mesmo resto na divisão por $25$ que os seus últimos dois algarismos.

### 3.2. Divisibilidade por $3$, $9$ e $11$

Os critérios de divisão por $3$, $9$ e $11$ são semelhantes entre si e seguem de um argumento semelhante aos critérios vistos anteriormente. Podemos ver essa semelhança a seguir.

**Proposição 25.** *Um número deixa o mesmo resto na divisão por $3$ que o número formado pela soma de seus algarismos.*

*Demonstração.* Seja $n \geq 0$ um inteiro escrito na base $10$ como $n = a_k a_{k-1} \dots a_1 a_0$. Como $10^j \equiv 1 \pmod 3$ para todo $j \geq 0$, temos

$$\begin{aligned} n &= a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 \\ &\equiv a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0 \pmod 3, \end{aligned}$$

como queríamos mostrar. □

Como $10^j \equiv 1 \pmod 9$, de forma completamente similar obtemos o seguinte critério.

**Proposição 26.** *Um número deixa o mesmo resto na divisão por $9$ que o número formado pela soma de seus algarismos.*

**Proposição 27.** *Um número deixa o mesmo resto na divisão por $11$ que o número formado pela soma de seus algarismos nas posições pares subtraído pela soma dos algarismos nas posições ímpares.*

*Demonstração.* Seja $n \geq 0$ um inteiro escrito na base $10$ como $n = a_k a_{k-1} \dots a_1 a_0$. Como $10 \equiv -1 \pmod{11}$, segue-se $10^j \equiv (-1)^j \pmod{11}$ para todo $j \geq 0$, temos

$$\begin{aligned} n &= a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0 \\ &\equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \cdots + a_2 - a_1 + a_0 \pmod{11}, \end{aligned}$$

como queríamos mostrar. □

### 3.3. Caso geral de divisibilidade

Nessa subseção, apresentamos os casos gerais dos critérios de divisibilidade. Começamos mostrando que se $r, s$ são coprimos e se temos um critério para divisibilidade por $r$ e um critério para divisibilidade por $s$, então temos um critério para o produto $rs$. Como consequência, se $d = p_1^{\alpha_1} \cdot \ldots \cdot p_t^{\alpha_t}$ é a fatoração de $d$ em potências de primos distintos, então basta ter um critério para cada potência de primo $p_i^{\alpha_i}$ para obtermos um critério de divisibilidade para $d$.

**Proposição 28.** *Sejam $r, s \geq 2$ inteiros coprimos. Então $rs \mid n$ se, e somente se, $r \mid n$ e $s \mid n$.*

*Demonstração.* $(\Rightarrow)$ Como $r \mid rs$ e $s \mid rs$, teremos $r \mid n$ e $s \mid n$.
$(\Leftarrow)$ Suponha que $r \mid n$ e $s \mid n$. Então existem $q_r$ e $q_s$ inteiros tais que $n = q_r r = q_s s$. Notemos que $r \mid q_s s$. Como $\mathrm{mdc}(r, s) = 1$, segue-se $r \mid q_s$. Logo existe $q$ inteiro tal que $q_s = qr$, portanto $n = qrs$ e assim $rs \mid n$. □

É possível usar o Teorema Chinês dos Restos, ver (MARTINEZ *et al.*, 2018, Teorema 2.2), para descobrir o resto da divisão de $n$ por $rs$ quando sabemos o resto da divisão de $n$ por $r$ e por $s$ separadamente.

Seja $n \in \mathbb{N}$. Da proposição anterior seguem os seguintes critérios que, a princípio, não preservam restos:

- Um número é divisível por $6$ se, e somente se, o número é divisível por $2$ e $3$.
- Um número é divisível por $24$ se, e somente se, o número é divisível por $3$ e $8$.
- Um número é divisível por $60$ se, e somente se, o número é divisível por $3$, $4$ e $5$.

Já construímos os critérios de divisibilidade para potências de $2$ e de $5$ na Subseção 3.1. Construiremos agora para as outras potências de primos. Seja $p$ um primo distinto de $2$ e de $5$ e seja $\alpha$ um inteiro positivo. Com isso, $\mathrm{mdc}(p^\alpha, 10) = 1$. Vejamos o critério de divisibilidade por $p^\alpha$.

**Teorema 29.** *Considere $q = \mathrm{ord}_{p^\alpha} 10$. Então $n$ deixa o mesmo resto na divisão por $d$ que a soma dos blocos de algarismos consecutivos de $n$ de tamanho $q$, isto é, se $n = a_{qk-1}10^{qk-1} + \cdots + a_1 10 + a_0$, então*

$$n \equiv (a_{kq-1} \cdots a_{k(q-1)})_{10} + (a_{2q-1} \cdots a_q)_{10} + \cdots + (a_{q-1} \cdots a_0)_{10} \pmod{d}.$$

*Demonstração.* Seja $n = a_{qk-1}10^{qk-1} + \cdots + a_0$ um inteiro escrito na base $10$. Podemos reescrever $n$ em blocos de $q$ algarismos:

$$n = (a_{kq-1} \cdots a_{k(q-1)})_{10} 10^{q(k-1)} + (a_{(k-1)q-1} \cdots a_{(k-2)q})_{10} 10^{q(k-2)} + \cdots + (a_{q-1} \cdots a_0)_{10}$$

Como $10^q \equiv 1 \pmod{d}$ temos então $10^{2q} \equiv 1, \cdots, 10^{(k-1)q} \equiv 1 \pmod{d}$. Daí, temos

$$\begin{aligned} n &= (a_{kq-1} \cdots a_{k(q-1)})_{10} 10^{q(k-1)} + \cdots + (a_{q-1} \cdots a_0)_{10} \\ &\equiv (a_{kq-1} \cdots a_{k(q-1)})_{10} + \cdots + (a_{q-1} \cdots a_0)_{10} \pmod{d}, \end{aligned}$$

como queríamos demonstrar. □

**Observação 30.** *Se a ordem $q$ é par, pode-se diminuir pela metade a quantidade de algarismos dos blocos a serem somados, mas a soma ficaria alternada. Isso ocorre pois teríamos $10^{q/2} \equiv -1 \pmod{p^\alpha}$.*

**Exemplo 31.** *Para ilustrar, vamos tomar* $d = 7$*, de forma que* $\mathrm{ord}_7 10 = 6$*. Pelo critério anterior,* $19181716151413121110987654321$ *é divisível por* $7$ *se, e somente se,* $654321+110987+413121+716151+19181 = 215896498$ *é divisível por* $7$*. Perceba que ainda podemos repetir o processo para obter um números ainda mais simples de se verificar. Pelo mesmo processo anterior,* $215896498$ *é divisivel por* $7$ *se, e somente se,* $896498 + 215 = 896713$ *é divisivel por* $7$*, o que é mais simples de verificar que o número inicial.*

Vamos ver agora um critério de divisibilidade pelo número $7$ que não preserva o resto.

**Proposição 32.** *Seja* $n \geq 1$ *um inteiro e* $y$ *seu algarismo das unidades, isto é, escrevemos* $n = 10x + y$*, onde* $x \geq 0$ *é o inteiro formado pelos outros algarismos de* $n$*. Então* $n$ *é divisível por* $7$ *se, e somente se,* $x - 2y$ *é divisível por* $7$*.*

*Demonstração.* Temos $7 \mid n \Leftrightarrow n \equiv 0 \pmod 7 \Leftrightarrow 3x + y \equiv 0 \pmod 7$. Multiplicando a congruência por $5$ obtemos $x + 5y \equiv 0 \pmod 7 \Leftrightarrow x - 2y \equiv 0 \pmod 7 \Leftrightarrow 7 \mid x - 2y$. □

**Exemplo 33.** *Retornaremos ao Exemplo 31 e tomaremos* $n = 896713$ *para verificar a sua divisibilidade por* $7$*. Pelo critério anterior, obtemos* $89665$*, aplicando sucessivamente temos os seguintes números:* $8956$, $883$, $82$ *e* $4$*. Como o* $4$ *não é divisível por* $7$*, concluímos que* $896713$ *não é divisível por* $7$*.*

Do Teorema 29 seguem os critérios de divisibilidade por $13$ e $37$ que exemplificaremos a seguir.

**Exemplo 34.** *Tomamos* $d = 13$*, de forma que* $\mathrm{ord}_{13} 10 = 6$*. O número* $75267252375005014812774$ *é divisível por* $13$ *se e somente se* $812774 + 5014 + 252375 + 75267 = 1145430$ *também é divisível por* $13$*.*

**Exemplo 35.** *Tomamos* $d = 37$*, de forma que* $\mathrm{ord}_{37} 10 = 3$*. O número* $5556804344814774853451$ *é divisível por* $37$ *se e somente se* $451 + 853 + 774 + 814 + 344 + 804 + 556 + 5 = 4601$ *também é divisível por* $37$*.*

**Observação 36.** *Note que nos Exemplos 34 e 35, é possível aplicar novamente os critérios de divisibilidade, de forma que a cada aplicação do critério obtemos um número ainda mais simples para verificar a divisão.*

Pelos Exemplos 34 e 35 podemos observar que quanto maior o valor da ordem de $q$ módulo $d$, maior é a dificuldade de encontrar o critério para esse número. As principais dificuldades são encontrar a ordem para um $d$ muito grande e manipular os cálculos de "blocos" de $q$ algarismos.

## 4. CONCLUSÃO

Em conclusão, os critérios de divisibilidade são ferramentas eficientes para resolver problemas de divisão. Embora poucos critérios sejam necessários ou práticos para serem usados diariamente, as propriedades que usamos para construir esses critérios não deixam de ser interessantes e computacionalmente viáveis. Além disso, os conceitos de congruência, ordem, máximo divisor comum e fatoração em primos nos permitem determinar teoricamente, de forma simples, critérios de divisibilidade por quaisquer números e expandir os critérios também para outras bases além da decimal.

## 5. AGRADECIMENTOS

Agradeço ao Programa de Educação Tutorial de Matemática (PETMAT-UFOP) pelo apoio na criação deste artigo. Também agradeço ao professor orientador Sávio Ribas, pela orientação nesse trabalho.

## 6. REFERÊNCIAS

MARTINEZ, F.; MOREIRA, C.; SALDANHA, N.; TENGAN, E. Teoria dos números: um passeio com primos e outros números. **IMPA, Rio de Janeiro, 5ª edição**, 2018.

SANTOS, J. P. d. O. **Introdução à teoria dos números**. [S.l.]: IMPA, 1998.