UNIVERSIDADE FEDERAL DO AMAPÁ

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL-PROFMAT

DENILSON PONTES BARBOSA AMANAJAS

DIVISIBILIDADE POR CONGRUÊNCIA

MACAPÁ-AP

2019

UNIVERSIDADE FEDERAL DO AMAPÁ

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL-PROFMAT

DENILSON PONTES BARBOSA AMANAJAS

DIVISIBILIDADE POR CONGRUÊNCIA

Dissertação apresentada ao Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal do Amapá - UNIFAP, como requisito necessário para obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. José Walter Cárdenas Sotil

MACAPÁ-AP

2019

Dados Internacionais de Catalogação na Publicação (CIP)
Biblioteca Central da Universidade Federal do Amapá
Elaborada por Orinete Costa Souza – CRB11/920

Amanajas, Denilson Pontes Barbosa.
Divisibilidade por congruência / Denilson Pontes Barbosa Amanajas ; Orientador, José Walter Cárdenas Sotil. – Macapá, 2019.
87 f.

Dissertação (Mestrado) – Fundação Universidade Federal do Amapá, Programa de Pós-Graduação em Matemática (PROFMAT).

1. Matemática – Estudo e ensino. 2. Algoritmo de divisibilidade. 3 Aprendizagem. 4. Matemática (Ensino fundamental). 5. Matemática (Ensino Médio). I. Sotil, José Walter Cárdenas, orientador. II. Fundação Universidade Federal do Amapá. III.Título.

510.7 A484d
CDD. 22 ed.

UNIVERSIDADE FEDERAL DO AMAPÁ

MESTRADO PROFSSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós Graduação Mestrado Profissional em Matemática em rede Nacional – PROFMAT, da Universidade Federal do Amapá – UNIFAP foram convocados para realizar a arguição da Dissertação de Mestrado de DENILSON PONTES BARBOSA AMANAJAS intitulada: **Divisibilidade por Congruência**, após terem inquerido o aluno e realizado avaliação do trabalho, são de parecer pela sua APROVAÇÃO no rito da defesa.

A outorga do título de Mestre está sujeita à homologação pelo colegiado, ao atendimento de todas as indicações e correções solicitadas pela Banca e ao pleno atendimento das demandas regimentais do Programa de Pós Graduação.

Macapá, 19 de junho de 2019.

DR. JOSÉ WALTER CÁRDENAS SÓTIL
Presidente da Banca Examinadora (UNIFAP)

Me. HILTON BRUNO PEREIRA VIANA
Avaliador Externo (IFAP)

Dr. ERASMO SENGER
Avaliador Interno (UNIFAP)

“Esse trabalho é dedicado aos meus filhos Gustavo Furtado Amanajas e Eduardo Furtado Amanajas, que compreenderam os momentos de ausência. Também dedico a minha esposa Michelle Souza Furtado, que sempre foi uma grande companheira me ajudando a tornar esse sonho possível”

AGRADECIMENTOS

Agradeço imensamente à Deus, por ter me concedido saúde, força e disposição para realizar o curso e o trabalho de conclusão. Sem ele, nada disso seria possível. Também sou grato por ter dado saúde aos meus familiares e tranquilizado o meu espirito nos momentos mais difíceis da minha trajetória acadêmica.

Aos meus pais, Francisco Barbosa Amanajas e Gercina Pontes Barbosa, pelo apoio, força e amor incondicional. Sem vocês a realização desse sonho não seria possível.

Sou grato a todos os professores que contribuíram com a minha formação, especialmente ao professor José Walter Cárdenas Sotil, responsável pela orientação do meu trabalho. Obrigado por esclarecer tantas dúvidas sendo paciente e atento aos mínimos detalhes.

A todos os amigos, meu muito obrigado. Aos momentos de descontração e motivação que vocês compartilharam comigo nessa etapa desafiadora da vida acadêmica.

E por fim, à instituição Universidade Federal do Amapá-UNIFAP, que ao longo da minha formação ofereceu um ambiente de estudo agradável e repleto de oportunidades.

“A tarefa não é tanto ver aquilo que ninguém viu, mas pensar o que ninguém ainda pensou sobre aquilo que todo mundo vê.”

(Arthur Schopenhauer)

RESUMO

O presente trabalho constitui uma abordagem diferenciada para o estudo de divisibilidade utilizando conhecimentos de congruência, tendo em vista a grande dificuldade de compreensão e aplicação deste conhecimento. Inicialmente menciona-se a constituição dos sistemas numéricos e os métodos utilizados para dividir dos povos Egípcios, Romanos e Hindus. As definições, proposições, teoremas e lemas constituem a fundamentação teórica necessária para efetuar procedimentos de divisibilidades. Através de análise dos referenciais teóricos, criou-se um recurso metodológico denominado algoritmo de divisibilidade por congruência (ADCG) utilizado para calcular divisibilidades e possibilitar ao aluno um novo recurso que contribui significativamente para processo de ensino e aprendizagem. Este recurso oportunizou construir uma proposta de ensino direcionado para alunos do ensino fundamental das séries finais e ensino médio com o objetivo de auxiliar, intensificar e melhorar o entendimento do conteúdo ministrado em sala de aula.

Palavras chave: Divisibilidade. Congruência. Algoritmo de divisibilidade. Proposta de ensino.

ABSTRACT

The present paper constitutes a differentiated approach for the divisibility study by using knowledge of congruence, considering the huge difficulty of understanding and application of this knowledge. Initially, the constitution of numerical systems and the methods used to divide from the Egyptian, Roman and Hindu peoples are mentioned. The definitions, propositions, theorems and mottos compose the theoretical basis needed to perform divisibility procedures. Through the analysis of theoretical reference, a methodological resource named congruence divisibility algorithm (GCDA) was created, used to calculate divisibilities and provide to the student a new resource that contributes significantly to the teaching and learning process. This resource brought the opportunity to construct a proposal of teaching directed to students of final levels of elementary education and high school, with the aim of assisting, intensifying and improving the understanding of the content taught in the classroom.

Keywords: divisibility. Congruence. Divisibility algorithm. Teaching proposal.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Os indícios relacionados a ideia da concepção de números surgiram a partir da necessidade de registrar quantidades em relações de contagem provenientes de insumos, dos quais, os povos utilizavam para sua sobrevivência.

Com o passar do tempo a necessidade de contar e estabelecer correspondência entre quantidades proporcionou ao homem a possibilidade de desenvolver símbolos capazes de expressar inúmeras situações. Estes símbolos seriam a origem dos números, que posteriormente, serviram para a construção de sistemas de numeração.

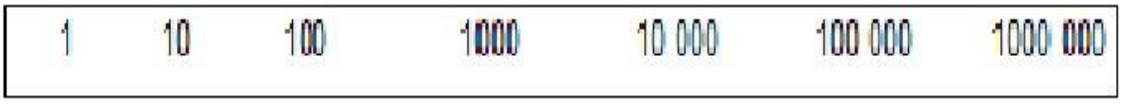
Esses sistemas foram criados, ao longo do tempo, em várias partes do mundo, oriundos do Antigo Egito e Babilônia. Segundo Tatiana Roque (2012):

> .... a referência ás necessidades práticas de cada um desses povos não basta para explicar a criação de diferentes sistemas de numeração, com regras próprias e bem distintas uma das outras. É preciso relativizar, portanto, a interpretação frequente de que a Matemática nesta época era construída somente por procedimentos de cálculo voltados para a resolução de problemas cotidianos. (p.8).

Os números tiveram suas origens com os povos egípcios, por volta de 3000 a.C, motivados pela necessidade de se realizar cálculos com mais agilidade e precisão, é importante mencionar que nesse período ocorreram muitos avanços na área da construção e a principal delas foram as pirâmides, pois o método até então utilizado através de número concreto representados por pedras, nós ou riscos em ossos não estava suprindo as necessidades da época. Foi quando surgiram as representações simbólicas através da quantidade de objetos que era apresentado por desenhos.

Eles organizaram seu sistema de numeração em sete quantidades, conforme figura 1.1.

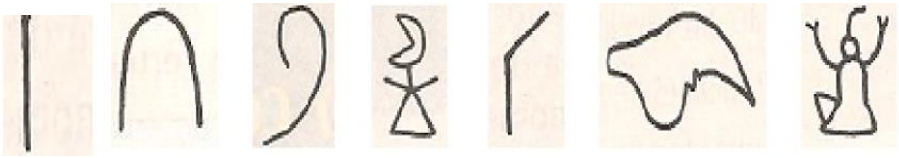
Figura 1.1 – Sistema de numeração Egípcio



Fonte: Matemática e os números naturais, 2019.

Estas quantidades eram representadas por símbolos (ver figura 1.2):

Figura 1.2 – Símbolos Egípcios



Fonte: Matemática e os números naturais, 2019.

Todos os números eram obtidos por meio da combinação dessas quantidades e uma característica importante é que a ordem dos símbolos não modificava o número.

Inicialmente os cálculos egípcios eram realizados por adições, com o passar do tempo surgiu a necessidade de compor números que representasse uma parte do todo. Em decorrência disso é que os egípcios criaram um novo tipo de número chamado de fracionário. Deste se utilizava apenas frações unitárias da forma $\frac{1}{n}$.

Os romanos por volta de 2000 a.C., organizaram os números de uma maneira mais eficiente. Eles não usaram novos símbolos para representá-los, utilizaram somente as letras do próprio alfabeto para compor os esses números. Baseavam-se em um sistema de numeração que era formado por sete valores e cada um representado por uma letra romana. Assim temos que:

- I: Assumia o valor 1 unidade.
- V: Assumia o valor 5 unidades.
- X: Assumia o valor 10 unidades.
- L: Assumia o valor 50 unidades.
- C: Assumia o valor 100 unidades.
- D: Assumia o valor 500 unidades.
- M: Assumia o valor 1000 unidades.

Os cálculos efetuados pelos romanos eram direcionados para as operações de adição e subtração. E neste contexto, pode-se perceber que os números formados dependem da ordem em que aparecem.

Este sistema de numeração foi utilizado por muitos outros povos, mas se percebia um detalhe importante, que era a dificuldade de se fazer cálculos com ele.

Foi então que surgiu, na Índia, uma das mais notáveis invenções de toda a história da Matemática. Um novo sistema de numeração decimal chamado de indo-

arábico que foi desenvolvido pelos hindus e transmitido pelos Árabes para toda a Europa ocidental.

Os primeiros vestígios foram encontrados na Índia nas colunas de pedras com data do ano 250 a.C., eram símbolos numéricos, sem a presença do zero, que representavam o início desse sistema de numeração. O símbolo zero “0” é a representação de uma notação para uma posição vazia e só se tem ocorrência dois séculos depois dos indícios dos nove outros dígitos.

A composição completa dos números incluindo o zero foi descrita no livro do matemático persa Al-Khowârizmî no ano de 825 d.C. Esta representação numérica foi introduzida na Europa inicialmente por Gerbert (950 – 1003), pois ele estudou em escolas mulçumanas da Espanha e posteriormente pelo Leonardo de Pisa através de seus trabalhos. A esse respeito, Boyer (2012) declara:

> ... A nova numeração, que chamamos em geral de sistema hindu, é apenas uma nova combinação de três princípios básicos, todos de origem antiga: (1) uma base decimal; (2) uma notação posicional; e (3) uma forma cifrada para cada um dos dez numerais. (p.155)

O sistema decimal utiliza dez símbolos chamados de algarismos e são definidos por: 0 – 1 – 2 – 3 – 4 – 5 – 6 – 7 – 8 – 9. Com estes símbolos pode-se formar infinitos números através de grupamentos.

- A cada dez unidades é formada uma dezena.
- A cada dez dezenas é formada uma centena.
- A cada dez centenas é formada um milhar.

Continuando este processo novos números serão obtidos com uma quantidade maior de algarismos, ou seja, a representação que corresponde a um número qualquer é composto de vários algarismos dispostos, uns a seguir aos outros. Os lugares destes algarismos correspondem às diferentes ordens, começando pela direita, e são chamados de casas: casa das unidades, casa das dezenas etc.

O sistema Indo-Arábico é definido como um sistema de posição, pois o valor do algarismo é determinado através da posição ocupada pelo numeral.

> No sistema decimal, o símbolo 0 (zero) posicionado à esquerda do número escrito não altera seu valor representativo. Assim: 1; 01; 001 ou 0001 representam a mesma grandeza, neste caso a unidade. O símbolo zero posto à direita implica em multiplicar a grandeza pela base, ou seja, por 10 (dez): 1, 10, 100, 1000, etc. (Mat. UFRGS,2008, p.3).

Como os números são formados por grupamentos de 10 em 10, um número qualquer neste sistema, pode ser escrito em potencias de base 10, como por exemplo:

- O número 7 pode ser escrito como: $7\text{x}10^0$
- O número 15 pode ser escrito como: $1\text{x}10^1 + 5\text{x}10^0$
- O número 103 pode ser escrito como: $1\text{x}10^2 + 0\text{x}10^1 + 3\text{x}10^0$

Generalizando, um número qualquer do sistema indo arábico pode ser escrito da forma:

$$n = a_n\text{x}10^n + a_{n-1}\text{x}10^{n-1} + a_{n-2}\text{x}10^{n-2} + \cdots + a_1\text{x}10^1 + a_0\text{x}10^0$$

Com esta forma representativa de numeração, se tornou muito mais fácil de escrever qualquer número, por maior que ele fosse, e como estes números foram criados com o propósito de tornar mais prático contar elementos da natureza, eles foram denominados como números naturais.

A grande quantidade de objetos a serem contados, assim como, as atividades práticas através de problemas oriundos de situações reais em cada época e o espírito indagador e questionador do homem foram cruciais para a determinação da noção de conjunto numérico.

O conjunto dos números naturais, baseado na noção de sucessor, é definido por meio de propriedades chamadas de axiomas. Giuseppe Peano (1858 – 1932) propõe, por meio de quatro axiomas, caracterizar a estrutura de uma sequência de números naturais.

> 1) Todo número natural possui um único sucessor, que também é um número natural.
> 2) Números naturais diferentes tem sucessores diferentes.
> 3) Existe um único número natural, designado por 1, que não é sucessor de nenhum outro.
> 4) Seja X um conjunto de números naturais (isto é $X \subset \text{N}$). Se $1 \in X$ e se,além disso, o sucessor de cada elemento de X ainda pertence a X, então $X = \text{N}$. (MORGADO, 2013, p. 2).

1.1 A DIVISÃO DOS EGÍPCIOS

A operação de divisão dos egípcios era realizada por meio de um processo de sucessivas duplicações, ou seja, o divisor é dobrado sucessivamente. Fato este, pautado na premissa de que todo número pode ser representado por uma soma de potência de base dois.

O processo se define através de uma tabela com duas colunas, na primeira coluna coloca-se duplicações a partir do número um e na segunda, duplicações a partir do divisor. É importante mencionar que não se utiliza o valor do dividendo nesta operação.

Exemplo. Efetuar a divisão de 130 por 5.

Solução;

Passo1. Inicialmente, constrói-se uma tabela com duas colunas. A primeira coluna com as duplicações a partir do número um, e a segunda coluna com as duplicações do valor 5 (divisor). Na primeira coluna, são inseridos os valores 1, 2, 4, 8, 16 e 32 que correspondem, respectivamente, as potências $2^0, 2^1, 2^2, 2^3$ e 2^5. Os números preenchidos na segunda coluna são 5, 10, 20, 40, 80 e 160. Estes, são valores duplicações a partir do divisor 5.

Tabela 1.1 – Duplicações.

Duplicações a partir do número 1(potências de base dois).	**Duplicações a partir do divisor 5**
$1=(2^0)$	5
$2=(2^1)$	10
$4=(2^2)$	20
$8=(2^3)$	40
$16=(2^4)$	80
$32=(2^5)$	160

Fonte: Revista eletrônica de Matemática, 2019.

Passo 2. Seleciona-se números da segunda coluna, podendo ser um ou mais, que quando somados seja igual ou mais próximo do valor 130, ou seja, o dividendo da operação. É importante observar que este processo de escolha dos números é único.

Passo 3. O resultado da soma dos números da primeira coluna, correspondentes aos números escolhidos no Passo 2, será o quociente.

Assim, a soma dos números 16 (correspondente a 80 na 2ª coluna), 8 (correspondente a 40 na 2ª coluna) e 2 (correspondente a 10 na 2ª coluna), resulta no valor 26 que é o quociente da divisão. Logo, 130 divido por 5 é igual a 26 (ver na tabela 1.1).

1.2 A DIVISÃO DOS ROMANOS

Para o povo romano, as operações de multiplicação e divisão não foram bem definidas ao longo da história. A seguir, são elencadas algumas situações de como se aplicava o processo de divisão para calcular a metade de um número.

Para se calcular a metade de um número, bastaria reduzir pela metade a quantidade de cada algarismo. Este tipo de operação, dependendo do valor numérico, pode ser efetuado através dos seguintes procedimentos:

1) Os algarismos que se apresentam em quantidades pares:

   A metade de II é I;

   A metade de XX é X;

   A metade de XXXX é XX;

   A metade de CCXX é CX.

2) Os algarismos podem ser representados por quantidades pares equivalentes:

   A metade de X= V V é V;

   A metade de XXX = XXVV é XV;

   A metade de D = CCCCLL é CCL.

3) Sendo um número par e apresentando V na sua escrita. Deve-se substituir V por IIIII.

   A metade de VI = IIIIII é III;

   A metade de XVI = VVIIIIII é VIII;

   A metade de CVIII = LLIIIIIIII é LIIII (ou LIV).

4) Para a divisão não exata, considera-se apenas a parte inteira do quociente, não importando o valor do resto.

   A metade de V = IIIII é II e resto I;

   A metade de XI = VVI é V e resto I;

1.3 A DIVISÃO DOS HINDUS

Para os hindus, que utilizavam o sistema decimal e posicional representado pelos algarismos 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9, o procedimento utilizado para calcular divisões era chamado de “método do galeão”, por sua semelhança com um navio. Este método consiste em dividir o dividendo pelos fatores do divisor.

Considera-se os seguintes passos da divisão de 44977 por 382:

Passo 1. Escreve-se o divisor à esquerda do dividendo. Depois obtém-se o primeiro algarismo do quociente $(449 : 382)$, que é 1 e logo em seguida será escrito à direita do dividendo conforme está descrito abaixo.

$$382 \quad | \quad 44977 \quad | \quad 1$$

Passo 2. Escreve-se o produto:1 x 382, que é 382, abaixo de 449.

- Calcula-se mentalmente: $4 - 3 = 1$. Em seguida riscam-se os algarismos 4 e 3 e escreve-se 1 acima do primeiro 4.
- Como não se pode subtrair 8 de 4, agrupa-se o 1, que foi escrito acima, com o 4 e calcula-se mentalmente: $14 - 8 = 6$. Depois riscam-se o 1, o 4 e o 8 e escreve-se 6 acima do segundo 4.
- Calcula-se mentalmente $9 - 2 = 7$. Em seguida riscam-se o 9 e o 2 e escreva 7 acima do 9.

$$382 \quad \left| \begin{array}{l} \cancel{1}67 \\ \cancel{449}77 \\ \cancel{382} \end{array} \right| \quad 1$$

Passo 3. O dividendo resultante do passo 2 é 6777, que são os algarismos não riscados, lidos de cima para baixo, na coluna do meio. Logo, obtém-se o próximo algarismo do quociente $(677 : 382)$, que resulta em 1.

- Escreve-se o produto definido por 1 x 382, que é 382, colocado o 3 abaixo do 8, o 8 abaixo do 2 e o 2 abaixo do 7.
- Calcula-se mentalmente $(6 - 3 = 3)$. Risca-se o 6, o 3 e em seguida escreve-se 3 acima do 6.
- Como não se pode subtrair 8 de 7, risque o 3 e escreva 2 acima do 3 e calcula-se mentalmente $(17 - 8 = 9)$. Riscam-se o 7 e o 8 e escreve-se 9 acima do 7.
- Calcula-se mentalmente $(7 - 2 = 5)$. Risca-se o 7 e o 2 e em seguida escreve-se 5 acima do 7.

$$\begin{array}{c|c|c} 382 & \begin{array}{c} 2 \\ \cancel{3}9 \\ \cancel{167}5 \\ \cancel{4497}7 \\ \cancel{3822} \\ \cancel{38} \end{array} & 11 \end{array}$$

Passo 4. O dividendo resultante do passo 3 é 2957, que são os algarismos não riscados, lidos de cima para baixo, na coluna do meio. Obtém-se o próximo algarismo do quociente ($2957 : 382$), que é 7.

- Escreve-se o produto definido por 7 x 382, que tem como resultado 2674, coloca-se o 2 abaixo do 3, o 6 abaixo do 8, o 7 abaixo do 2 e o 4 abaixo do 7.
- Calcula-se mentalmente $2 - 2 = 0$. Riscam-se os dois algarismos 2.
- Calcula-se mentalmente $9 - 6 = 3$. Riscam-se o 9 e o 6 e escreve-se o 3 acima do 9.
- Como não se pode subtrair 7 de 5, risca-se o 3 e escreve-se 2 acima do 3. Calcula-se mentalmente $15 - 7 = 8$. Riscam-se o 5 e o 7 e escreve-se 8 acima do 5.
- Calcula-se mentalmente $7 - 4 = 3$. Riscam-se o 7 e o 4 e escreve-se 3 acima do 7.

$$\begin{array}{c|c|c} 382 & \begin{array}{c} 2 \\ \cancel{23} \\ \cancel{39}8 \\ \cancel{1675}3 \\ \cancel{44977} \\ \cancel{38224} \\ \cancel{387} \\ \cancel{26} \end{array} & 117 \end{array}$$

Passo 5. O quociente é 117 e o resto é 283.

1.4 OS ELEMENTOS DE EUCLIDES

Euclides foi dos maiores matemáticos da história e autor de notáveis livros denominados os elementos. Este consistia em treze livros que eram dedicados a:

1. Geometria plana através dos estudos de triângulos, linhas paralelas, propriedades do círculo;
2. Geometria espacial através dos estudos de construções no espaço, prismas, cones, esferas e poliedros regulares.
3. O algoritmo de Euclides é consiste em um método simples e eficaz de determinar o máximo divisor comum entre dois números inteiros diferente de zero por meio de divisões sucessivas.

No próximo capítulo serão definidas algumas propriedades relacionadas a divisibilidade e as implicações de cada uma. Números primos com definições e propriedades.

2 FUNDAMENTAÇÃO TEÓRICA

A divisão representa uma das quatro operações fundamentais da aritmética. Este processo ocorre através do ato de dividir, ou separar, uma determinada quantidade em partes iguais. O número que está sendo dividido em partes iguais é denominado dividendo e o número que indica em quantas vezes dividir é definido como divisor.

Segundo os autores Oliveira (2006) e Pereira da silva (2015), as propriedades que fundamentam a divisibilidade podem ser descritas da seguinte forma:

Definição 2.1. *Dados $a, b \in \mathbb{Z}$, com $a \neq 0$, dizemos que a divide b, denotamos por $a|b$, se existir um $k \in \mathbb{Z}$* , tal que $b = a.k$. Caso a não divida b, escrevemos $a \nmid b$.

Exemplo 2.1. Verificar as possíveis divisões de:

a) 60 por 5;
b) 20 por 3.

Solução:

a) Como 60 pode ser escrito através da multiplicação de$5 \cdot 12$, e sendo $5 \neq 0$ com $12 \in \mathbb{Z}$. Tem-se que $60 = 5 \cdot 12$, portanto $5|60$.
b) Como 20 pode ser escrito através das multiplicações de $1 \cdot 20$, $2 \cdot 10$, $4 \cdot 5$. Em nenhuma das possibilidades aparece o número 3 como um elemento do produto para determinar o valor 20. Conclui-se que $3 \nmid 20$.

A seguinte proposição mostra que a relação de divisibilidade (|) é transitiva.

Proposição 2.1. *Se a, b e $c \in \mathbb{Z}$, $a|b$ e $b|c$, então $a|c$.*

Demonstração**:**

Por hipótese $a|b\ e\ b|c$, então pela Definição 2.1 existem $k_1, k_2 \in \mathbb{Z}$ tal que $b = a \cdot k_1$ e $c = b \cdot k_2$. Substituindo o valor de b na equação $c = b \cdot k_2$ teremos $c = a \cdot k_1 \cdot k_2$ como $k_1, k_2 \in \mathbb{Z}$ implica que $a|c$.■

Exemplo 2.2: Sejam $a = 3, b = 12,\ e\ c = 48$, como $3|12$ e $12|48$ então $3|48$.

A relação de divisibilidade verifica que o divisor divide a combinação linear de dois dividendos, como mostra a seguinte proposição.

Proposição 2.2. *Se $a, b, c, m\ e\ n \in \mathbb{Z}$, $c|a\ e\ c|b$, então $c|(m \cdot a \pm n \cdot b)$.*

Demonstração:

Por hipótese $c|a\ e\ c|b$, então pela Definição 2.1 existem $k_1, k_2 \in \mathbb{Z}$ tal que $a = c \cdot k_1$ e $b = c \cdot k_2$. Multiplicando-se estas duas equações respectivamente por m e n teremos $m \cdot a = m \cdot c \cdot k_1$ e $n \cdot b = n \cdot c \cdot k_2$. Somando-se membro a membro obtemos $m \cdot a + n \cdot b = c \cdot (m \cdot k_1 + n \cdot k_2)$, ou seja, $c|(m \cdot a + n \cdot b)$. De maneira análoga provamos que $c|(m \cdot a - n \cdot b)$.■

Exemplo 2.3. Seja $a = 12, b = 6\ e\ c = 3$, $m = 2\ e\ n = 5$, como $3|12$ e $3|6$ então $3|(2 \cdot 12 + 5 \cdot 6)$.

2.1 ALGORITMO DA DIVISÃO

A divisão euclidiana permite escrever o dividendo como o produto do divisor pelo quociente mais um resto, como descrito pelo seguinte teorema.

Teorema 2.1. *Dados $a\ e\ b \in \mathbb{Z}$, com $b \neq 0$, existem únicos $q\ e\ r \in \mathbb{Z}$ tais que*

$a = b \cdot q + r,$ *com* $0 \leq r < |b|, (r = 0 \Leftrightarrow b|a),$ onde os inteiros q *e* r *são respectivamente, o quociente e resto da divisão de a por b.*

Demonstração:

i) Suponha primeiro que $b > 0$, e seja q o maior inteiro tal que $b \cdot q \leq a$. Então $b \cdot q \leq a < b \cdot (q+1) = b \cdot q + b$, de modo que $0 \leq a - b \cdot q < b$ e basta definir $r = a - b \cdot q$.

ii) se $b < 0$, então $-b > 0$, donde existem $q, r \in \mathbb{Z}$ tais que $a = (-b) \cdot q + r$, com $0 \leq r < -b = |b|$.

Desta forma, temos garantida, a existência de q e r.

A fim de mostrarmos a unicidade, suponha a existência de outro par $q' e\, r' \in \mathbb{Z}$, verificando: $a = b \cdot q + r = b \cdot q' + r'$, com $0 \leq r' < |b|$.

Disto tem-se

$(b \cdot q + r) - (b \cdot q' + r') = 0 \Rightarrow b \cdot (q - q') = r' - r$,

ou seja, $b|(r' - r)$.

Mas, como $r' < b$ e $r < b$, tem-se $|r' - r| < b$ e, como $b|(r' - r)$ deve-se ter

$r' - r = 0$ o que implica $r' = r$.

Logo, $q' \cdot b = q \cdot b \Rightarrow q = q'$, uma vez que $b \neq 0$.■

É importante observar que se o resto da divisão de a por b, sendo $a, b \in \mathbb{Z}$, for zero, significa dizer que $b|a$.

O Teorema 2.1 possibilita determinar o quociente e o resto de uma divisão através de subtrações sucessivas utilizando o dividendo e divisor. Este processo é conhecido como algoritmo da divisão.

Exemplo 2.4. Calcular o quociente e resto da divisão de 32 por 5.

Solução:

Utilizando o algoritmo da divisão $a - b \cdot q = r$, com $r < b$, tem-se:

$$32 - 5 \cdot 1 = 27 \qquad (27 \not< 5)$$

$$32 - 5 \cdot 2 = 22 \qquad (22 \not< 5)$$

$$32 - 5 \cdot 3 = 17 \qquad (17 \not< 5)$$

$$32 - 5 \cdot 4 = 12 \qquad (12 \not< 5)$$

$$32 - 5 \cdot 5 = 7 \qquad (7 \not< 5)$$

$$32 - 5 \cdot 6 = 2 \qquad (2 < 5) \qquad \text{PARAR}$$

Satisfeita a condição $r < b$,ou seja, $2 < 5$. O quociente da divisão de 32 por 5 é 6 e o resto é 2.

2.2 MÁXIMO DIVISOR COMUM (M.D.C).

O máximo divisor comum é um procedimento executável o qual permite calcular o maior divisor que se pode obter entre dois números, ou seja, é o maior inteiro que divide ambos os números sem deixar resto. Assim, se define o M.D.C:

Definição 2.2. *O máximo divisor comum de dois inteiros a e b, não simultaneamente nulos, denotado por (a, b), é o maior inteiro positivo que divide a e b.*

Exemplo 2.5. Determinar o máximo divisor comum dos números 16 e 20.

Solução:

Inicialmente será determinado os divisores de 16 e 18. Assim, tem-se:

$$D(16) = \{1,2,\mathbf{4},8,16\}$$

$$D(20) = \{1,2,\mathbf{4},5,10,20\}$$

O maior divisor comum aos dois números é o 4. Logo, o $M.D.C\ (16,20) = 4$.

Um dos mais antigos (aproximadamente 300 anos a.C) método matemático utilizado para se determinar o máximo divisor comum é chamado de algoritmo de Euclides. Pode ser encontrado no Livro VII da obra *Os Elementos e* continua sendo uma das maneiras mais simples e eficientes de se calcular o M.D.C. Este é obtido a partir de divisões sucessivas e se desenvolve utilizando os seguintes passos:

Passo 1. Primeiramente, efetua-se a divisão de a por b, com $0 < b < a$ representado através a expressão $a = b \cdot q_1 + r_1$, com $0 \leq r_1 < b$ e escreve-se os valores no diagrama:

	q_1	
a	b	
r_1		

Passo 2. A seguir, efetua-se a divisão de b por r_1, com $r_1 < b$. Representado através da expressão $b = r_1 \cdot q_2 + r_2$, com $0 \leq r_2 < q_2$, e escreve-se os valores no diagrama:

	q_1	q_2	
a	b	r_1	
	r_1	r_2	

Passo 3. Prosseguindo, o processo de divisão, enquanto for possível, até que se obtenha:

	q_1	q_2	q_3	$\cdots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	$r_n = (a, b)$
	r_1	r_2	r_3	$\cdots$	r_n	0	

Exemplo 2.6. Calcular o M.D.C dos números 1128 e 336.

Solução:

Aplicando o algoritmo de Euclides obtém-se:

	3	2	1	4
1128	336	120	96	24
120	96	24	0	

Logo, o mdc (1128,336) = 24

Definição 2.3. *Os inteiros a e b são relativamente primos quando $(a, b) = 1$.*

Exemplo 2.7. Verificar se os números 550 e 21 são primos entre si.

Solução:

Para resolver esse problema é necessário determinar o M.D.C entre os números 550 e 21. Assim, aplicando o algoritmo de Euclides tem-se:

	26	5	4
550	21	4	1
4	1	0	

Logo, como o $M.D.C(550,21) = 1$. Eles são primos entre si.

O teorema a seguir define que o máximo divisor comum de dois números inteiros pode ser escrito como uma combinação linear destes com coeficientes numéricos inteiros. Esta afirmação é chamada de Teorema de Bézout.

Teorema 2.2. *Seja $d \in \mathbb{Z}$ o máximo divisor comum de a e $b \in \mathbb{Z}$, então existem inteiros n_0 e $m_0 \in \mathbb{Z}$ tais $d = n_0 \cdot a + m_0 \cdot b$.*

Demonstração

Seja B o conjunto de todas as combinações lineares $n \cdot a + m \cdot b$ onde n e $m \in \mathbb{Z}$.

Este conjunto contém claramente, números negativos, positivos e também o zero.

Sejam n_0 e m_0 tal que $c = n_0 \cdot a + m_0 \cdot b$ é o menor inteiro positivo pertencente ao conjunto B. Mostraremos que $c|a$ e $c|b$.

Suponhamos que $c \nmid a$. Neste caso, pelo teorema 2.1, existem q e r tais que:

$$a = q \cdot c + r \quad \text{com} \quad 0 < r < c$$

Portanto,

$$r = a - q \cdot c = a - q \cdot (n_0 \cdot a + m_0 \cdot b) = a \cdot (1 - q \cdot n_0) + (-q \cdot m_0) \cdot b$$

Isto mostra que $r \in B$, pois $(1 - q \cdot n_0)$ e $(-q \cdot m_0) \in \mathbb{Z}$, o que é uma contradição, uma vez que $0 < r < c$ e c é o menor elemento positivo de B.

Logo, $c|a$ e de forma análoga se prova que $c|b$.

Como d é um divisor comum de a e b, existem k_1 e $k_2 \in \mathbb{Z}$, tais que $a = k_1 \cdot d$ e $b = k_2 \cdot d$ e, portanto $c = n_0 \cdot a + m_0 \cdot b = n_0 \cdot k_1 \cdot d + m_0 \cdot k_2 \cdot d = d \cdot (n_0 \cdot k_1 + m_0 \cdot k_2)$ o que implica que $d|c$ e como $d < c$ não é possível, uma vez que d é o maior divisor comum.

Logo conclui-se que $d = n_0 \cdot a + m_0 \cdot b$.■

Se o produto de dois números primos entre si divide um número inteiro qualquer. Esses valores que fazem parte do produto também são divisores do inteiro.

Teorema 2.3. *Dados d, m e $n \in \mathbb{Z}$, tal que $d = m \cdot n$ e $(m,n) = 1$, então $d|a$, com $a \in \mathbb{Z}$, se, e somente se, $m|a$ e $n|a$.*

Demonstração

- ⇒) Como $d|a$, pela Definição 2.1, existe um $r \in \mathbb{Z}$ tal que $a = d \cdot r$, mas por hipótese $d = m \cdot n$, donde $a = m \cdot n \cdot r$, o que implica que $m|a$ e $n|a$.

- ⇐) Como $m|a$ e $n|a$, pela Definição 2.1, existem $r_1, r_2 \in \mathbb{Z}$, tal que

  $$a = m \cdot r_1 \text{ e } a = n \cdot r_2 \qquad (I)$$

  como por hipótese $(m,n) = 1$ e $d = m \cdot n$, segue-se do teorema 2.2 que:

- $m \cdot b + n \cdot c = 1$ (multiplicando ambos os membros por a)
- $m \cdot b \cdot a + n \cdot c \cdot a = a$ (substituindo (I) na parte esquerda da igualdade)
- $m \cdot b \cdot n \cdot r_2 + n \cdot c \cdot m \cdot r_1 = a$
- $m \cdot n \cdot (b \cdot r_2 + c \cdot r_1) = a \Rightarrow m \cdot n | a \Rightarrow d | a$. ■

Se um número inteiro qualquer é divisor de um produto de dois outros números em que um destes dois é primo com o divisor. Então aquele que não é primo também é divisível pelo divisor.

Teorema 2.4. *Sejam a, b e $c \in \mathbb{Z}$. Se $a | b \cdot c$ e $(a, b) = 1$, então $a | c$.*

Demonstração

Como $(a, b) = 1$ pelo Teorema 2.2 existem inteiros n e m tais que $n \cdot a + m \cdot b = 1$. Multiplicando – se os dois lados desta igualdade por c, se obtém:

$$n \cdot (a \cdot c) + m \cdot (b \cdot c) = c.$$

Como $a | a \cdot c$ e, por hipótese, $a | b \cdot c$ então, pela Proposição 2.2, $a | c$. ■

Se entre dois números inteiros distintos, um é divisor do outro. Então o máximo divisor comum entre eles é o próprio divisor.

Teorema 2.5. *Dados $a, b \in \mathbb{Z}$, $a | b \Leftrightarrow (a, b) = a$*

Demonstração

- $\Rightarrow$) Se $a | b$, então pela definição 2.1 existe $k \in \mathbb{Z}$ tal que $b = a \cdot k$ onde $(a, b) = (a, a \cdot k) = a$, pois $(1, k) = 1$
- $\Leftarrow$) Se $(a, b) = a \Rightarrow a | a$ e $a | b$. ■

2.3 NÚMEROS PRIMOS

O termo “primo”, em matemática, indica a ideia de primeiro. Isto significa que esses números são responsáveis por gerar os demais números naturais por meio da operação de multiplicação. Logo, pode-se afirmar que todos os números naturais, que não são primos, podem ser escritos como um produto de números primos.

Definição 2.4. *Um inteiro $p > 1$ é primo se seus únicos divisores positivos forem 1 e p. Se o inteiro $n > 1$ não é primo dizemos que n é composto, ou seja, n pode ser fatorado num produto $n = b \cdot c$, onde $b, c > 1$ são inteiros.*

Exemplos 2.8.

a) O número 2 tem apenas dois divisores o 1 e 2, portanto 2 é um número primo;
b) O número 19 tem apenas dois divisores o 1 e 19, portanto 19 é um número primo;
c) O número 15 possui os divisores 1, 3, 5 e 15, portanto 15 não é primo. Logo, é composto;
d) O número 20 possui os divisores 1, 2, 4, 5, 10 e 20, portanto 20 não é primo. Logo, é composto

Se um número inteiro é primo e divide um produto de dois outros números. Então esse número primo é divisor de um desses números que fazem parte do produto.

Proposição 2.3. *Sejam a, b e $p \in \mathbb{Z}$. Se $p|a \cdot b$, p primo, então $p|a$ ou $p|b$.*

Demonstração

Se $p \nmid a$, então $(a, p) = 1$ o que implica, pelo Teorema 2.4, $p|b$.■

Todo número inteiro diferente de -1, 0 e 1 pode ser expresso como um produto de números primos, de forma única, a menos da ordem dos fatores. Esse resultado, é denominado como ***Teorema fundamental da Aritmética***, descrito no livro IX dos *Elementos* de Euclides e evidencia a importância dos números primos na Teoria dos números.

Teorema 2.6. *Todo inteiro $n > 1$ pode ser representado de maneira única, a menos da ordem dos fatores, como um produto de fatores primos.*

Demonstração

- Se n é primo não há nada a demonstrar.
- Suponhamos, pois n composto. Seja $p_1 > 1$ o menor divisor positivo de n. Afirmamos que p_1 é primo. Isto é verdade, pois, caso contrário existiria p, $1 < p < p_1$ com $p|n$, contradizendo a escolha de p_1. Logo $n = p_1 \cdot n_1$.
- Se n_1 for primo a prova está completa. Caso contrário, tomamos p_2 como menor fator de n_1. Pelo argumento anterior, p_2 é primo e temos que $n = p_1 \cdot p_2 \cdot n_2$.

  Repetindo este procedimento, obtemos uma sequência decrescente e inteiros positivos $n_1, n_2, n_3, \dots, n_r$. Como todos eles são inteiros maiores que 1, este processo deve terminar. Como os primos na sequência $p_1, p_2, p_3, \dots, p_k$ não são necessariamente, distintos n terá, em geral, a forma:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k}$$

  Para mostrarmos a unicidade usamos a indução em n.

- Para $n = 2$ a, afirmação é verdadeira.
- Assumimos, então, que ela se verifica para todos os inteiros maiores que 1 e menores que n. Vamos provar que ela é também verdadeira para n.
- Se n for primo, não há nada a provar.
- Vamos supor, então, que n seja composto e que tenha duas fatorações, isto é:

$$n = p_1 p_2 p_3 \dots . p_s = q_1 q_2 q_3 \dots q_r$$

- Vamos provar que $s = r$ e que cada p_i é igual a algum q_j. Como p_i divide o produto $q_1 q_2 q_3 \dots q_r$ ele divide pelo menos um dos fatores q_j. Sem perda de generalidade podemos supor que $p_1|q_1$. Logo $\frac{n}{q_1} = p_2 p_3 \dots p_s = q_2 q_3 \dots q_r$. Como $1 < \frac{n}{p_1} < n$, a hipótese de indução nos diz que as duas fatorações são idênticas, isto é,$s = r$ e a menos da ordem, as fatorações $p_1 p_2 p_3 \dots . p_s$ e $q_1 q_2 q_3 \dots q_r$ são iguais.■

Lema 2.1. (Euclides). *Todo inteiro $n > 1$ pode ser escrito como um produto de um número finito de primos não necessariamente distintos.*

Demonstração:

Por indução. Se $n = 2$, nada há a fazer, pois 2 é primo. Suponhamos que todo inteiro n tal que $2 \leq n < m$ pode ser escrito como um produto de um número finito de primos; provemos que este também é o caso para m:

Se m for primo, nada há de fazer. Caso não seja, existem inteiros a e b tais que $m = a \cdot b$, com $1 < a, b < m$. Pela hipótese de indução, a e b podem ser escritos como um produto de números finitos de primos, escrevemos $a = p_1 p_2 \dots p_k$, $b = q_1 q_2 \dots q_l$, com $k, i \geq 1$ e $p_1, \dots, p_k, q_1, \dots, q_l$ primos,.

Logo, $m = a \cdot b = p_1 \dots p_k q_1 \dots q_l$, também um produto finito de primos.■

Exemplo 2.9.

Um processo prático elementar usado para decompor um número qualquer em fatores primos segue como base o Teorema 2.6 e Lema 2.1. Por exemplo, para n =90, obtem-se:

90	2
45	3
15	3
5	5
1	

Logo, $90 = 2 \cdot 3^2 \cdot 5$

Para qualquer sequência finita de números primos, sempre haverá um número primo que não está presente na sequência.

Teorema 2.7. (Euclides). *A sequência de números primos é infinita.*

Demonstração:

Vamos supor que a sequência dos primos seja finita.

Seja pois, $p_1, p_2, \dots, p_n$ a lista de todos os primos.

Considerando o número $R = p_1 p_2 \ldots p_n + 1$, é claro que R não é divisível por nenhum dos p_i da lista e que R é maior que qualquer p_i.

Mas, pelo Teorema 2.6, ou R é primo ou possui algum fator primo e isto implica na existência de um primo que não pertence a essa lista. Portanto a sequência dos números primos não pode ser finita.■

Exemplo 2.10.

a) Se considerarmos que todos os números primos conhecidos fossem 2,3 e 5. Calculando o número p dado por $p = 2 \cdot 3 \cdot 5 + 1$. Obtém-se $p = 31$. O valor de p não é divisível por 2, nem por 3, nem por 5 pois tal divisão deixaria resto 1. Logo, p é primo ou é composto. Como 31 é primo então p é primo.

b) Se considerarmos, agora, que todos os números primos conhecidos fossem 2, 3, 5, 7, 11 e 13. Calculando o número p dado por $p = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1$. Obtém-se $p = 30031$. Utilizando o algoritmo de Euclides chega-se ao seguinte resultado: $30031 = 59\text{x}509$. Portando encontra-se dois números primos 59 e 509 que não estavam na sequência conhecida.

Neste próximo capítulo será apresentado propriedades relacionadas a congruência módulo m. As definições, proposições, lemas e teoremas constituem a fundamentação necessária para desenvolver procedimentos de resolução das divisibilidades através do uso de congruência.

3 CONGRUÊNCIAS

Neste capítulo será apresentado uma importante ferramenta da Teoria Elementar dos números denominado congruência. Parte deste conhecimento foi introduzido pelo matemático alemão Carl Friedrich Gauss (1777 – 1855) em um trabalho publicado em 1801 chamado *Disquistiones Arithmeticae*.

A congruência possui muitas aplicações importantes. Dentre elas, a justificativa para critérios de divisibilidade, exemplificação de conceitos que envolvem as propriedades das operações, construção de códigos e no estudo e modelagem de fenômenos periódicos que envolvem diferentes campos do conhecimento como: matemática (teoria dos jogos, teoria dos grafos), física, artes, música e etc...

3.1 CONGRUÊNCIA MÓDULO M

A congruência módulo m é uma relação de equivalência no conjunto dos números inteiros de tal forma que dados dois inteiros a e b, a é congruente a b módulo m, onde m é um número inteiro positivo, se e somente se, a diferença $a - b$ for divisível por m. Assim:

Definição 3.1. *Sejam a, b e m inteiros dados, sendo $m > 1$, dizemos que a é congruente a b, modulo m, denotamos $a \equiv b \ (mod\ m)$, se $m|(a - b)$. Se $m \nmid (a - b)$ dizemos que a é incongruente a b modulo m e denotamos $a \not\equiv b \ (modulo\ m)$.*

Exemplo 3.1.

- $21 \equiv 15 \ (mod\ 6)$, pois $6|(21 - 15)$. Observa-se que o resto da divisão dos dois números por 6 é igual a 3.
- Como $7 \nmid 9$ e $9 = 32 - 23$ temos que $32 \not\equiv 23 \ (mod\ 7)$.

A congruência módulo m entre dois números inteiros pode ocorrer quando, nesta operação, aparecer um terceiro inteiro tal que o primeiro seja igual a soma do segundo mais o produto do terceiro com o valor m.

Proposição 3.1. *Se a e b são inteiros, temos que $a \equiv b\ (mod\ m)$ se, e somente se, existir um inteiro k tal que $a = b + km$.*

Demonstração

- ⇒) Se $a \equiv b\ (mod\ m)$, então $m|(a - b)$ o que implica na existência de um inteiro k tal que $a - b = km$, isto é, $a = b + km$.
- ⇐) A reciproca é trivial pois a existência de um k satisfazendo $a = b + km$, temos $km = a - b$, ou seja, que $m|(a - b)$ isto é, $a \equiv b\ (mod\ m)$.

Exemplo 3.2. Se $43 \equiv 28\ (mod\ 5)$, então $5|(43 - 28)$. Como $43 = 28 + 3 \cdot 5$, isto implica em $43 - 28 = 3 \cdot 5$.

Esta proposição estabelece que a relação de congruência, definida no conjunto dos inteiros, é uma relação de equivalência. Pois mediante a demonstração dos itens a seguir, verifica-se que elas são, reflexiva, simétrica e transitiva.

Proposição 3.2. *Se a, b, m e d são inteiros, $m > 0$, as seguintes sentenças são verdadeiras:*

1. $a \equiv a\ (mod\ m)$ (reflexiva)
2. Se $a \equiv b\ (mod\ m)$, então $b \equiv a\ (mod\ m)$ (simétrica)
3. Se $a \equiv b\ (mod\ m)$ e $b \equiv c\ (mod\ m)$, então $a \equiv c\ (mod\ m)$ (transitiva).

Demonstração

1. Como $m|0$, então $m|(a - a)$, o que implica $a \equiv a\ (mod\ m)$.

2. Se $a \equiv b\ (mod\ m)$, então $a = b + k_1 m$ para algum inteiro k_1. Logo $b = a - k_1 m$ o que implica na Proposição 3.1, $b \equiv a\ (mod\ m)$.

3. Se $a \equiv b\ (mod\ m)$ e $b \equiv d\ (mod\ m)$, então existem inteiros k_1 e k_2 tias que $a - b = k_1 m$ e $b - d = k_2 m$. Somando-se, membro a membro, estas últimas equações, obtemos $a - d = (k_1 + k_2) \cdot m$, o que implica $a \equiv d\ (mod\ m)$.■

Exemplo 3.3.

a) Se $5|0$, então $5|(7-7)$. Logo $7 \equiv 7\ (mod\ 5)$;

b) Se $29 \equiv 5\ (mod\ 8)$, então tem-se que $29 = 5 + (3)8$. Logo, escrevendo $5 = 29 + (-3) \cdot 8$, com $-3 \in \mathbb{Z}$, obtém-se $5 \equiv 29\ (mod\ 8)$;

c) Se $31 \equiv 3\ (mod\ 7)$ e $3 \equiv 66\ (mod\ 7)$, então têm-se que $31 - 3 = (4)7\ (I)$ e $3 - 66 = (-9)7\ (II)$. Somando (I) e (II) obtém-se $31 - 66 = \big(4 + (-9)\big)7 = (-5)7$ o que implica em $31 \equiv 66\ (mod\ 7)$.

A utilização de congruência modular é muito útil para resolução de problemas com números inteiros, pois pelo fato de ser uma relação de equivalência, é possível aplicar as operações de adição e multiplicação.

Teorema 3.1. *Se a, b, c e m são inteiros tais que $a \equiv b\ (mod\ m)$, então:*

1. $a + c \equiv b + c\ (mod\ m)$
2. $a - c \equiv b - c\ (mod\ m)$
3. $a \cdot c \equiv b \cdot c\ (mod\ m)$

Demonstração

1. Como $a \equiv b\ (mod\ m)$, temos que $a - b = km$ e, portanto, como $a - b = (a + c) - (b + c)$ temos $a + c \equiv b + c\ (mod\ m)$.

2. Como $(a - c) - (b - c) = a - b$ e, por hipótese, $a - b = km$ temos que $a - c \equiv b - c\ (mod\ m)$.

3. Como $a - b = km$ então $a \cdot c - b \cdot c = c \cdot km$ o que implica $m|\ (ac - bc)$ e, portanto, $a \cdot c \equiv b \cdot c\ (mod\ m)$.

Exemplo 3.4.

1. Se $36 \equiv 12\ (mod\ 8)$, então $36 - 12 = 3 \cdot 8$. Como $36 - 12 = (36 + 10) - (12 + 10)$ temos $36 + 10 \equiv 12 + 10\ (mod\ 8)$.

2. Se $(49 - 6) - (28 - 6) = 49 - 28$ e $49 - 28 = 21 = 3 \cdot 7$, então temos que $(49 - 6) \equiv (28 - 6)(mod\ 7)$.

3. Se $54 - 34 = 2 \cdot 10$, então $54 \cdot 8 - 34 \cdot 8 = 8 \cdot 2 \cdot 10$ o que implica que $10|(54 \cdot 8 - 34 \cdot 8)$ e, portanto $54 \cdot 8 \equiv 34 \cdot 8\ (mod\ 10)$

Uma vez estabelecida a congruência entre dois números inteiros. Essa relação se mantem para qualquer valor obtido a partir da potência desses inteiros elevados a uma mesmo expoente.

Proposição 3.3. Se a, b, k e m são inteiros com $k > 0$ e $a \equiv b\ (mod\ m)$, então

$a^k \equiv b^k\ (mod\ m)$.

Demonstração

Da fatoração $a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + ab^{k-2} + b^{k-1})$.

E como $m|(a - b)$, segue da Definição 3.1 que $m|(a^k - b^k)$.

Logo $a^k \equiv b^k\ (mod\ m)$.

Exemplo 3.5 Calcular o resto da divisão 2^{50} por 7.

Solução

Como $2^3 \equiv 8\ (mod\ 7)$ e $8 \equiv 1\ (mod\ 7)$, segue da Proposição 3.2 que:

$$2^{48} \equiv (2^3)^{16} \equiv 8^{16} \equiv 1^{16} \equiv 1\ (mod\ 7)$$

Assim, temos que

$$2^{48} \equiv 1\ (mod\ 7) \qquad \text{(I)}.$$

Aplicando o Teorema 3.1 em (I), obtemos:

$$2^2 \cdot 2^{48} \equiv 2^2 \cdot 1\ (mod\ 7)$$

$$2^{50} \equiv 4\ (mod\ 7)$$

Logo, $2^{50} \equiv 4\ (mod\ 7)$, ou seja, a divisão de 2^{50} por 7 deixa resto 4.

O teorema a seguir fornece um teste de não primalidade, ou seja, estabelece uma verificação, por meio da utilização de divisibilidade por congruência, se um número inteiro é primo ou não.

Teorema 3.2. (Pequeno Teorema de Fermat) *Seja p primo. Se $p \nmid a$ então* $a^{p-1} \equiv 1\ (mod\ p)$.

Demonstração

O conjunto formado pelos p números $0,1,2,\dots,p-1$ constiui um sistema completo de resíduos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjunto de $\{0,1,2,\dots,p-1\}$.

Vamos, agora, considerar os números $a \cdot i, 1 \leq i \leq p-1$ os quais não são divisíveis por p, ou seja, nenhum é congruente a zero módulo p.

Quaisquer dois deles são incongruentes módulo p, pois $aj \equiv ak\ (mod\ p)$ implica $j \equiv k\ (mod\ p)$ isto só é possível se $j = k$, uma vez que ambos j e k são positivos e menores que p.

Temos, portanto, um conjunto de $p-1$ elementos incongruentes módulo p e não divisíveis por p. Logo, cada um deles é congruente a exatamente um dentre os elementos $1,2,3,\dots,p-1$.

Se multiplicarmos essas congruências, teremos:

$a(2a)(3a)\dots(p-1)a \equiv 1.2.3\dots(p-1)\ (mod\ p)$,

ou seja,

$a^{p-1}(p-1)! \equiv (p-1)!\ (mod\ p)$.

Mas, como $\big((p-1)!, p\big) = 1$, podemos cancelar o fator $(p-1)!$ em ambos os lados, obtendo $a^{p-1} \equiv 1\ (mod\ p)$. ■

Exemplo 3.6. Verificar se o número 3^{34} é divisível por 11.

Solução

Como $11 \nmid 3$, pois o $mdc(3,11) = 1$ e sendo 11 primo aplica-se o teorema 3.2. Assim:

$$3^{11-1} \equiv 1\ (mod\ 11)$$

$$3^{10} \equiv 1\ (mod\ 11)\ \ (I)$$

Utilizando a proposição 3.3 em (I) segue:

$$(3^{10})^3 \equiv 1^3\ (mod\ 11)$$

$$3^{30} \equiv 1\ (mod\ 11)\ \ (II)$$

Se $3^4 = 81$ e $81 \equiv 4\ (mod 11)$ então $3^4 \equiv 4\ (mod\ 11)\ \ (III)$. Usando o teorema 3.1 em (II) e (III) obtem-se:

$$3^{30} \cdot 3^4 \equiv 1 \cdot 4\ (mod\ 11)$$

$$3^{34} \equiv 4\ (mod\ 11)$$

Logo, 3^4 não é divisível por 11, pois deixa resto 4.

Corolário 3.1. *Se p é um primo e a é um inteiro positivo, então $a^p \equiv a\ (mod\ p)$.*

Demonstração

Temos que analisar dois casos, se $p|a$ e se $p \nmid a$.

- Se $p|a$, então $p|(a(a^{p-1} - 1))$ e, portanto $a^p \equiv a\ (mod\ p)$.
- Se $p \nmid a$, pelo Teorema 2.10 $p|(a^{p-1} - 1)$ e, portanto, $p|(a^p - a)$.

Logo, em ambos os casos, $a^p \equiv a\ (mod\ p)$.■

Exemplo 3.7. Verificar se 26^{42} é divisível por 13.

Solução

Seja $26^{42} = 26^{3.13+3} = (26^{13})^3 \cdot 26^3$. Como $13|26$ e sendo 13 primo aplica-se o corolário 3.1. Assim:

$$26^{13} \equiv 26\ (mod\ 13)\ \ (I)$$

Utilizando a proposição 3.3 em (I), segue:

$$(26^{13})^3 \equiv 26^3\ (mod\ 13)$$

$$26^{39} \equiv 26^3 \ (mod\ 13) \ \ (II)$$

Se $26 \equiv 0 \ (mod\ 13)$ e $26^3 \equiv 0^3 \ (mod\ 13)$ então $26^3 \equiv 0 \ (mod\ 13) \ \ (IIi)$. Usando o teorema 3.1 em (II) e (III) obtém-se:

$$26^{39} \cdot 26^3 \equiv 26^3 \cdot 0 \ (mod\ 13)$$

$$26^{42} \equiv 0 \ (mod\ 13)$$

Logo, o número 26^{42} é divisível por 13.

4 DIVISIBILIDADE POR CONGRUÊNCIA

Neste capítulo, será mostrado como se aplica os conhecimentos de congruência para provar se um determinado número é divisível por outro, ou seja, se a divisão de um número qualquer por outro deixa resto, sendo ele primo ou não.

Propomos neste trabalho uma forma prática de analisar a divisibilidade usando congruências, usando o seguinte algoritmo:

4.1 ALGORITMO DA DIVISIBILIDADE POR CONGRUÊNCIAS (ADCG)

Dado os números naturais D e d, para analisar se d divide D, se constrói uma matriz, seguindo o seguinte procedimento:

i) Decompomos D na forma:

$$D = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$$

ii) Calculamos para cada elemento a_i os restos na congruência módulo d

$$a_i \equiv r_i \ \ (mod\ d), \quad i = 1, \cdots, n \qquad (I)$$

Os restos r_i são colocados na primeira linha da matriz

iii) Calculamos para cada elemento b_i os restos na congruência módulo d

$$b_i \equiv s_i \ \ (mod\ d), \quad i = 1, \cdots, n \qquad (II)$$

Os restos s_i são colocados na segunda linha da matriz

iv) Como

$$a_i b_i \equiv r_i\, s_i \ \ (mod\ d), \quad i = 1, \cdots, n \qquad (III)$$

A terceira linha é formada pelo produto dos elementos da mesma coluna das linhas 1 e 2.

v) Como

$$r_i\, s_i \equiv z_i \ \ (mod\ d), \quad i = 1, \cdots, n \qquad (IV)$$

A quarta linha é formada pelos restos obtidos a partir resultado do produto da terceira linha.

vi) Como

$$D = a_1 b_1 + \cdots + a_{nb_n} \equiv r_1\, s_1 + \cdots r_n s_n \equiv z_1 + \cdots z_n \ \ (mod\ d), \qquad (V)$$

Esta soma dos restos é colocada na última coluna da matriz. Se for necessário se faz uma última equivalência para que a soma seja menor que d.

vii) Se o resto em V) é zero concluímos que d divide D, caso contrário d não divide D.

viii) A matriz toma a seguinte forma

Tabela 4.1 – Valores obtidos através da congruência modulo d do número D.

(I)	r_1	r_2	...	r_n	(V) TOTAL
(II)	s_1	s_2	...	s_n	
(III) Produto	r_1s_1	r_2s_2	...	r_ns_n	
(IV) Resto	z_1	z_2	...	z_n	z_1+ ...+z_n

Fonte: Autor

A vantagens do algoritmo ADCG são:

- Se d não divide D, o algoritmo calcula o resto da divisão, o qual não é calculado pelos métodos da divisibilidade
- Não é necessário lembrar um conjunto de regras de divisibilidade para cada número. Geralmente o aluno tende a esquecer estas regras.
- O algoritmo trabalha no aprimoramento do uso das congruências pelo aluno, conceito importante em várias áreas do conhecimento.

4.2 DIVISIBILIDADE POR 2

Exemplo 4.1. Verificar se o número 4637 é divisível por 2.

Solução

A divisão pode ser definida como:

$$4637 \equiv \_ \ (mod\ 2)$$

Sendo $4637 = 4 \cdot 10^3 + 6 \cdot 10^2 + 3 \cdot 10^1 + 7 \cdot 10^0$, temos:

$$4 \cdot 10^3 + 6 \cdot 10^2 + 3 \cdot 10^1 + 7 \cdot 10^0 \equiv \_ \ (mod\ 2)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 4 \equiv 0\ (mod\ 2) \\ 6 \equiv 0\ (mod\ 2) \\ 3 \equiv 1\ (mod\ 2) \\ 7 \equiv 1\ (mod\ 2) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^3 \equiv 0^3 \equiv 0\ (mod\ 2) \\ 10^2 \equiv 0^2 \equiv 0\ (mod\ 2) \\ 10^1 \equiv 0\ (mod\ 2) \\ 10^0 \equiv 1\ (mod\ 2) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.2 – Valores obtidos através da congruência modulo 2 do número 4637.

(I)	0	0	1	1	(V) TOTAL
(II)	0	0	0	1	
(III) Produto	0x0 = 0	0x0 = 0	1x0 = 0	1x1 = 1	
(IV) Resto	0	0	0	1	1

Fonte: Autor

Logo, teremos:

$$4637 \equiv 1\ (mod\ 2)$$

Portanto, o número 4637 não é divisível por 2, pois deixa resto 1.

Exemplo 4.2. Verificar se o número 524 é divisível por 2.

Solução

A divisão pode ser definida como:

$$524 \equiv \_\ (mod\ 2)$$

Sendo $524 = 5 \cdot 10^2 + 2 \cdot 10^1 + 4 \cdot 10^0$, temos:

$$5 \cdot 10^2 + 2 \cdot 10^1 + 4 \cdot 10^0 \equiv \_\ (mod\ 2)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 5 \equiv 1\ (mod\ 2) \\ 2 \equiv 0\ (mod\ 2) \\ 4 \equiv 0\ (mod\ 2) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^2 \equiv 0^2 \equiv 0\ (mod\ 2) \\ 10^1 \equiv 0\ (mod\ 2) \\ 10^0 \equiv 1\ (mod\ 2) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.3 – Valores obtidos através da congruência modulo 2 do número 524.

(I)	1	0	0	(V) TOTAL
(II)	0	0	1	
(III) Produto	1x0 = 0	0x0 = 0	0x1 = 0	
(IV) Resto	0	0	0	0

Fonte: Autor

Logo, teremos:

$$524 \equiv 0\ (mod\ 2)$$

Portanto, o número 524 é divisível por 2, pois deixa resto 0.

4.3 DIVISIBILIDADE POR 3

Exemplo 4.3. Verificar se o número 67 é divisível por 3.

Solução

A divisão pode ser definida como:

$$67 \equiv \_\ (mod\ 3)$$

Sendo $67 = 6 \cdot 10^1 + 7 \cdot 10^0$, temos:

$$6 \cdot 10^1 + 7 \cdot 10^0 \equiv \_\ (mod\ 3)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 6 \equiv 0\ (mod\ 3) \\ 7 \equiv 1\ (mod\ 3) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{matrix} 10^1 \equiv 1\ (mod\ 3) \\ 10^0 \equiv 1\ (mod\ 3) \end{matrix}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.4 – Valores obtidos através da congruência modulo 3 do número 67.

(I)	0	1	(V) TOTAL
(II)	1	1	
(III) Produto	0x1 = 0	1x1 = 1	
(IV) Resto	0	1	1

Fonte: Autor

Logo, teremos:

$$67 \equiv 1\ (mod\ 3)$$

Portanto, o número 67 não é divisível por 3, pois deixa resto 1.

Exemplo 4.4. Verificar se o número 732 é divisível por 3.

Solução

A divisão pode ser definida como:

$$732 \equiv \_\ (mod\ 3)$$

Sendo $732 = 7 \cdot 10^2 + 3 \cdot 10^1 + 2 \cdot 10^0$, temos:

$$7 \cdot 10^2 + 3 \cdot 10^1 + 2 \cdot 10^0 \equiv \_\ (mod\ 3)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{matrix} 7 \equiv 1\ (mod\ 3) \\ 3 \equiv 0\ (mod\ 3) \\ 2 \equiv 2\ (mod\ 3) \end{matrix}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{matrix} 10^2 \equiv 1^2 \equiv 1\ (mod\ 3) \\ 10^1 \equiv 1\ (mod\ 3) \\ 10^0 \equiv 1\ (mod\ 3) \end{matrix}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.5 – Valores obtidos através da congruência modulo 3 do número 732.

(I)	1	0	2	(V) TOTAL
(II)	1	1	1	
(III) Produto	1x1 = 1	0x1 = 0	2x1 = 2	
(IV) Resto	1	0	2	3

Fonte: Autor

Logo, teremos:

$$732 \equiv 3 \equiv 0\ (mod\ 3)$$

Portanto, o número 732 é divisível por 3, pois deixa resto 0.

4.4 DIVISIBILIDADE POR 4

Exemplo 4.5. Verificar se o número 5763 é divisível por 4.

Solução

A divisão pode ser definida como:

$$5763 \equiv \_\ (mod\ 4)$$

Sendo $5763 = 5 \cdot 10^3 + 7 \cdot 10^2 + 6 \cdot 10^1 + 3 \cdot 10^0$, temos:

$$5 \cdot 10^3 + 7 \cdot 10^2 + 6 \cdot 10^1 + 3 \cdot 10^0 \equiv \_\ (mod\ 4)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 5 \equiv 1\ (mod\ 4) \\ 7 \equiv 3\ (mod\ 4) \\ 6 \equiv 2\ (mod\ 4) \\ 3 \equiv 3\ (mod\ 4) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^3 \equiv 2^3 \equiv 2^2 \cdot 2 \equiv 0 \cdot 2 \equiv 0\ (mod\ 4) \\ 10^2 \equiv 2^2 \equiv 0\ (mod\ 4) \\ 10^1 \equiv 2\ (mod\ 4) \\ 10^0 \equiv 1\ (mod\ 4) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.6 – Valores obtidos através da congruência modulo 4 do número 5763.

(I)	1	3	2	3	(V) TOTAL
(II)	0	0	2	1	
(III) Produto	1x0 = 0	3x0 = 0	2x2 = 4	3x1 = 3	
(IV) Resto	0	0	4	3	7

Fonte: Autor

Logo, teremos:

$$5763 \equiv 7 \equiv 3\ (mod\ 4)$$

Portanto, o número 5763 não é divisível por 4, pois deixa resto 3.

Exemplo 4.6. Verificar se o número 31892 é divisível por 4.

Solução

A divisão pode ser definida como:

$$31892 \equiv \_\ (mod\ 4)$$

Sendo $31892 = 3 \cdot 10^4 + 1 \cdot 10^3 + 8 \cdot 10^2 + 9 \cdot 10^1 + 2 \cdot 10^0$, temos:

$$3 \cdot 10^4 + 1 \cdot 10^3 + 8 \cdot 10^2 + 9 \cdot 10^1 + 2 \cdot 10^0 \equiv \_\ (mod\ 4)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 3 \equiv 3\ (mod\ 4) \\ 1 \equiv 1\ (mod\ 4) \\ 8 \equiv 0\ (mod\ 4) \\ 9 \equiv 1\ (mod\ 4) \\ 2 \equiv 2\ (mod\ 4) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^4 \equiv 2^4 \equiv 2^2 \cdot 2^2 \equiv 0 \cdot 0 \equiv 0\ (mod\ 4) \\ 10^3 \equiv 2^3 \equiv 2^2 \cdot 2 \equiv 0 \cdot 2 \equiv 0\ (mod\ 4) \\ 10^2 \equiv 2^2 \equiv 4 \equiv 0\ (mod\ 4) \\ 10^1 \equiv 2\ (mod 4) \\ 10^0 \equiv 1\ (mod 4) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.7 – Valores obtidos através da congruência modulo 4 do número 31892.

(I)	1	3	0	1	2	(V) TOTAL
(II)	0	0	0	2	1	
(III) Produto	1x0 = 0	3x0 = 0	0x0 = 0	1x2 = 2	2x1 = 2	
(IV) Resto	0	0	0	2	2	4

Fonte: Autor

Logo, teremos:

$$31892 \equiv 4 \equiv 0\ (mod\ 4)$$

Portanto, o número 31892 é divisível por 4, pois deixa resto 0.

4.5 DIVISIBILIDADE POR 5

Exemplo 4.7. Verificar se o número 638 é divisível por 5.

Solução

A divisão pode ser definida como:

$$638 \equiv \_\ (mod\ 5)$$

Sendo $638 = 6 \cdot 10^2 + 3 \cdot 10^1 + 8 \cdot 10^0$, temos:

$$6 \cdot 10^2 + 3 \cdot 10^1 + 8 \cdot 10^0 \equiv \_\ (mod\ 5)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 6 \equiv 1\ (mod\ 5) \\ 3 \equiv 3\ (mod\ 5) \\ 8 \equiv 3\ (mod\ 5) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^2 \equiv 0^2 \equiv 0\ (mod\ 5) \\ 10^1 \equiv 0\ (mod\ 5) \\ 10^0 \equiv 1\ (mod\ 5) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.8 – Valores obtidos através da congruência modulo 5 do número 638.

(I)	1	3	3	(V) TOTAL
(II)	0	0	1	
(III) Produto	1x0 = 0	3x0 = 0	3x1 = 3	
(IV) Resto	0	0	3	3

Fonte: Autor

Logo, teremos:

$$638 \equiv 3\ (mod\ 5)$$

Portanto, o número 638 não é divisível por 5, pois deixa resto 3.

Exemplo 4.8. Verificar se o número 93075 é divisível por 5.

Solução

A divisão pode ser definida como:

$$93075 \equiv \_\ (mod\ 5)$$

Sendo $93075 = 9 \cdot 10^4 + 3 \cdot 10^3 + 0 \cdot 10^2 + 7 \cdot 10^1 + 5 \cdot 10^0$, temos:

$$9 \cdot 10^4 + 3 \cdot 10^3 + 0 \cdot 10^2 + 7 \cdot 10^1 + 5 \cdot 10^0 \equiv \_\ (mod\ 5)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 9 \equiv 4\ (mod\ 5) \\ 3 \equiv 3\ (mod\ 5) \\ 0 \equiv 0\ (mod\ 5) \\ 7 \equiv 2\ (mod\ 5) \\ 5 \equiv 0\ (mod\ 5) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^4 \equiv 0^4 \equiv 0\ (mod\ 5) \\ 10^3 \equiv 0^3 \equiv 0\ (mod\ 5) \\ 10^2 \equiv 0^2 \equiv 0\ (mod\ 5) \\ 10^1 \equiv 0\ (mod\ 5) \\ 10^0 \equiv 1\ (mod\ 5) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.9 – Valores obtidos através da congruência modulo 5 do número 93075.

(I)	4	3	0	2	0	(V) TOTAL
(II)	0	0	0	0	1	
(III) Produto	4x0 = 0	3x0 = 0	0x0 = 0	2x0 = 0	0x1 = 0	
(IV) Resto	0	0	0	0	0	0

Fonte: Autor

Logo, teremos:

$$93075 \equiv 0\ (mod\ 5)$$

Portanto, o número 93075 é divisível por 5, pois deixa resto 0.

4.6 DIVISIBILIDADE POR 6

Exemplo 4.9. Verificar se o número 102 é divisível por 6.

Solução

A divisão pode ser definida como:

$$102 \equiv \_\ (mod\ 6)$$

Sendo $102 = 1 \cdot 10^2 + 0 \cdot 10^1 + 2 \cdot 10^0$, temos:

$$1 \cdot 10^2 + 0 \cdot 10^1 + 2 \cdot 10^0 \equiv \_\ (mod\ 6)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 1 \equiv 1\ (mod\ 6) \\ 0 \equiv 0\ (mod\ 6) \\ 2 \equiv 2\ (mod\ 6) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^2 \equiv 4^2 \equiv 16 \equiv 4\ (mod\ 6) \\ 10^1 \equiv 4\ (mod\ 6) \\ 10^0 \equiv 1\ (mod\ 6) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.10 – Valores obtidos através da congruência modulo 6 do número 102.

(I)	1	0	2	(V) TOTAL
(II)	4	4	1	
(III) Produto	4x1 = 4	0x4 = 0	2x1 = 2	
(IV) Resto	4	0	2	6

Fonte: Autor

Logo, teremos:

$$102 \equiv 6 \equiv 0\ (mod\ 6)$$

Portanto, o número 102 é divisível por 6, pois deixa resto 0.

Exemplo 4.10. Verificar se o número 9347 é divisível por 6.

Solução

A divisão pode ser definida como:

$$9347 \equiv \_\ (mod\ 6)$$

Sendo $9347 = 9 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10^1 + 7 \cdot 10^0$, temos:

$$9 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10^1 + 7 \cdot 10^0 \equiv \_\ (mod\ 6)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 9 \equiv 3\ (mod\ 6) \\ 3 \equiv 3\ (mod\ 6) \\ 4 \equiv 4\ (mod\ 6) \\ 7 \equiv 1\ (mod\ 6) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^3 \equiv 4^3 \equiv 4^2 \cdot 4 \equiv 4 \cdot 4 \equiv 16 \equiv 4\ (mod\ 6) \\ 10^2 \equiv 4^2 \equiv 16 \equiv 4\ (mod\ 6) \\ 10^1 \equiv 4\ (mod\ 6) \\ 10^0 \equiv 1\ (mod\ 6) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.11 – Valores obtidos através da congruência modulo 6 do número 9347.

(I)	3	3	4	1	(V) TOTAL
(II)	4	4	4	1	
(III) Produto	3x4 = 12	3x4 = 12	4x4 = 16	1x1 = 1	
(IV) Resto	0	0	4	1	5

Fonte: Autor

Logo, teremos:

$$9347 \equiv 5\ (mod\ 6)$$

Portanto, o número 9347 não é divisível por 6, pois deixa resto 5.

1) **Observação:**

Pode-se obter valores negativos dos restos através do uso de congruência módulo m. O resto negativo é determinado subtraindo o número pelo valor da base e isto é utilizado quando o resto negativo é menor que o resto positivo em módulo.

4.7 OUTRA SOLUÇÃO UTILIZANDO RESTO NEGATIVO

A divisão pode ser definida como:

$$9347 \equiv \_\ (mod\ 6)$$

Sendo $9347 = 9 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10^1 + 7 \cdot 10^0$, temos:

$$9 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10^1 + 7 \cdot 10^0 \equiv \_\ (mod\ 6)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 9 \equiv 3\ (mod\ 6) \\ 3 \equiv 3\ (mod\ 6) \\ 4 \equiv -2\ (mod\ 6) \\ 7 \equiv 1\ (mod\ 6) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^3 \equiv 4^3 \equiv 4^2 \cdot 4 \equiv (-2) \cdot (-2) \equiv 4 \equiv -2\ (mod\ 6) \\ 10^2 \equiv 4^2 \equiv 16 \equiv 4 \equiv -2\ (mod\ 6) \\ 10^1 \equiv 4 \equiv -2\ (mod\ 6) \\ 10^0 \equiv 1\ (mod\ 6) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.12 – Valores obtidos através de restos positivos e negativos da congruência modulo 6 do número 9347.

(I)	3	3	-2	1	(V) TOTAL
(II)	-2	-2	-2	1	
(III) Produto	3x(-2) = -6	3x(-2) = -6	(-2)x(-2) = 4	1x1 = 1	
(IV) Resto	0	0	4	1	5

Fonte: Autor

Logo, teremos:

$$9347 \equiv 5\ (mod\ 6)$$

Portanto, o número 9347 não é divisível por 6, pois deixa resto 5.

4.8 DIVISIBILIDADE POR 7

Exemplo 4.11. Verificar se o número 326 é divisível por 7.

Solução

A divisão pode ser definida como:

$$326 \equiv \_\ (mod\ 7)$$

Sendo $326 = 3 \cdot 10^2 + 2 \cdot 10^1 + 6 \cdot 10^0$, temos:

$$3 \cdot 10^2 + 2 \cdot 10^1 + 6 \cdot 10^0 \equiv \_\ (mod\ 7)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 3 \equiv 3\ (mod\ 7) \\ 2 \equiv 2\ (mod\ 7) \\ 6 \equiv 6\ (mod\ 7) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^2 \equiv 3^2 \equiv 9 \equiv 2\ (mod\ 7) \\ 10^1 \equiv 3\ (mod\ 7) \\ 10^0 \equiv 1\ (mod\ 7) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.13 – Valores obtidos através da congruência modulo 7 do número 326.

(I)	3	2	6	(V) TOTAL
(II)	2	3	1	
(III) Produto	3x2 = 6	2x3 = 6	6x1 = 6	
(IV) Resto	6	6	6	18

Fonte: Autor

Logo, teremos:

$$326 \equiv 18 \equiv 4\ (mod\ 7)$$

Portanto, o número 326 não é divisível por 7, pois deixa resto 4.

Exemplo 4.12. Verificar se o número 248738 é divisível por 7.

Solução

A divisão pode ser definida como:

$$248738 \equiv \_\ (mod\ 7)$$

Sendo $248738 = 2 \cdot 10^5 + 4 \cdot 10^4 + 8 \cdot 10^3 + 7 \cdot 10^2 + 3 \cdot 10^1 + 8 \cdot 10^0$, temos:

$$2 \cdot 10^5 + 4 \cdot 10^4 + 8 \cdot 10^3 + 7 \cdot 10^2 + 3 \cdot 10^1 + 8 \cdot 10^0 \equiv \_\ (mod\ 7)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 2 \equiv 2\ (mod\ 7) \\ 4 \equiv 4\ (mod\ 7) \\ 8 \equiv 1\ (mod\ 7) \\ 7 \equiv 0\ (mod\ 7) \\ 3 \equiv 3\ (mod\ 7) \\ 8 \equiv 1\ (mod\ 7) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^5 \equiv 3^5 \equiv 3^4 \cdot 3^1 \equiv 4 \cdot 3 \equiv 12 \equiv 5\ (mod\ 7) \\ 10^4 \equiv 3^4 \equiv 3^2 \cdot 3^2 \equiv 2 \cdot 2 \equiv 4\ (mod\ 7) \\ 10^3 \equiv 3^3 \equiv 3^2 \cdot 3 \equiv 2 \cdot 3 \equiv 6\ (mod\ 7) \\ 10^2 \equiv 3^2 \equiv 9 \equiv 2\ (mod\ 7) \\ 10^1 \equiv 3\ (mod\ 7) \\ 10^0 \equiv 1\ (mod\ 7) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.14 – Valores obtidos através da congruência modulo 7 do número 248738.

(I)	2	4	1	0	3	1	(V) TOTAL
(II)	5	4	6	2	3	1	
(III) Produto	2x5 = 10	4x4 = 16	1x6 = 6	0x2=0	3x3=9	1x1=1	
(IV) Resto	3	2	6	0	2	1	14

Fonte: Autor

Logo, teremos:

$$248738 \equiv 14 \equiv 0\ (mod\ 7)$$

Portanto, o número 248738 é divisível por 7, pois deixa resto 0.

4.9 OUTRA SOLUÇÃO UTILIZANDO RESTO NEGATIVO

A divisão pode ser definida como:

$$248738 \equiv \_\ (mod\ 7)$$

Sendo $248738 = 2 \cdot 10^5 + 4 \cdot 10^4 + 8 \cdot 10^3 + 7 \cdot 10^2 + 3 \cdot 10^1 + 8 \cdot 10^0$, temos:

$$2 \cdot 10^5 + 4 \cdot 10^4 + 8 \cdot 10^3 + 7 \cdot 10^2 + 3 \cdot 10^1 + 8 \cdot 10^0 \equiv \_\ (mod\ 7)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 2 \equiv 2\ (mod\ 7) \\ 4 \equiv -3\ (mod\ 7) \\ 8 \equiv 1\ (mod\ 7) \\ 7 \equiv 0\ (mod\ 7) \\ 3 \equiv 3\ (mod\ 7) \\ 8 \equiv 1\ (mod\ 7) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^5 \equiv 3^5 \equiv 3^3 \cdot 3^2 \equiv (-1) \cdot 2 \equiv -2\ (mod\ 7) \\ 10^4 \equiv 3^4 \equiv 3^2 \cdot 3^2 \equiv 2 \cdot 2 \equiv 4\ \equiv -3 (mod\ 7) \\ 10^3 \equiv 3^3 \equiv 3^2 \cdot 3 \equiv 2 \cdot 3 \equiv 6 \equiv -1\ (mod\ 7) \\ 10^2 \equiv\ 3^2 \equiv 9 \equiv 2\ (mod 7) \\ 10^1 \equiv 3\ (mod\ 7) \\ 10^0 \equiv 1\ (mod\ 7) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.15 – Valores obtidos através de restos positivos e negativos da congruência modulo 7 do número 248738.

(I)	2	-3	1	0	3	1	(V) TOTAL
(II)	-2	-3	-1	2	3	1	
(III) Produto	2x(-2) = -4	(-3)x(-3) = 9	1x(-1) = -1	0x2=0	3x3=9	1x1=1	
(IV) Resto	-4	2	-1	0	2	1	0

Fonte: Autor

Logo, teremos:

$$248738 \equiv 0\ (mod\ 7)$$

Portanto, o número 248738 é divisível por 7, pois deixa resto 0.

4.10 DIVISIBILIDADE POR 8

Exemplo 4.13. Verificar se o número 952 é divisível por 8.

Solução

A divisão pode ser definida como:

$$952 \equiv \_\ (mod\ 8)$$

Sendo $952 = 9 \cdot 10^2 + 5 \cdot 10^1 + 2 \cdot 10^0$, temos:

$$9 \cdot 10^2 + 5 \cdot 10^1 + 2 \cdot 10^0 \equiv \_\ (mod\ 8)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 9 \equiv 1\ (mod\ 8) \\ 5 \equiv 5\ (mod\ 8) \\ 2 \equiv 2\ (mod\ 8) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^2 \equiv 2^2 \equiv 4\ (mod\ 8) \\ 10^1 \equiv 2\ (mod\ 8) \\ 10^0 \equiv 1\ (mod\ 8) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.16 – Valores obtidos através da congruência modulo 8 do número 952.

(I)	1	5	2	(V) TOTAL
(II)	4	2	1	
(III) Produto	1x4=4	5x2=10	2x1=2	
(IV) Resto	4	2	2	8

Fonte: Autor

Logo, teremos:

$$952 \equiv 8 \equiv 0\ (mod\ 8)$$

Portanto, o número 952 é divisível por 8, pois deixa resto 0.

Exemplo 4.14. Verificar se o número 34586 é divisível por 8.

Solução

A divisão pode ser definida como:

$$34586 \equiv \_\ (mod\ 8)$$

Sendo $34586 = 3 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 8 \cdot 10^1 + 6 \cdot 10^0$, temos:

$$3 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 8 \cdot 10^1 + 6 \cdot 10^0 \equiv \_\ (mod\ 8)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 3 \equiv 3\ (mod\ 8) \\ 4 \equiv 4\ (mod\ 8) \\ 5 \equiv 5\ (mod\ 8) \\ 8 \equiv 0\ (mod\ 8) \\ 6 \equiv 6\ (mod\ 8) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^4 \equiv 2^3 \cdot 2^1 \equiv 0 \cdot 2 \equiv 0\ (mod\ 8) \\ 10^3 \equiv 2^3 \equiv 2^2 \cdot 2 \equiv 4 \cdot 2 \equiv 8 \equiv 0\ (mod\ 8) \\ 10^2 \equiv 2^2 \equiv 4\ (mod\ 8) \\ 10^1 \equiv 2\ (mod\ 8) \\ 10^0 \equiv 1\ (mod\ 8) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.17 – Valores obtidos através da congruência modulo 8 do número 34586.

(I)	3	4	5	0	6	(V) TOTAL
(II)	0	0	4	2	1	
(III) Produto	3x0=0	4x0=0	5x4=20	0x2=0	6x1=6	
(IV) Resto	0	0	4	0	6	10

Fonte: Autor

Logo, teremos:

$$34586 \equiv 10 \equiv 2\ (mod\ 8)$$

Portanto, o número 34586 não é divisível por 8, pois deixa resto 2.

4.11 OUTRA SOLUÇÃO UTILIZANDO RESTO NEGATIVO

A divisão pode ser definida como:

$$34586 \equiv \_\ (mod\ 8)$$

Sendo $34586 = 3 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 8 \cdot 10^1 + 6 \cdot 10^0$, temos:

$$3 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 8 \cdot 10^1 + 6 \cdot 10^0 \equiv \_\ (mod\ 8)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 3 \equiv 3\ (mod\ 8) \\ 4 \equiv 4\ (mod\ 8) \\ 5 \equiv -3\ (mod\ 8) \\ 8 \equiv 0\ (mod\ 8) \\ 6 \equiv -2\ (mod\ 8) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^4 \equiv 2^3 \cdot 2^1 \equiv 0 \cdot 2 \equiv 0\ (mod\ 8) \\ 10^3 \equiv 2^3 \equiv 2^2 \cdot 2 \equiv 4 \cdot 2 \equiv 8 \equiv 0\ (mod\ 8) \\ 10^2 \equiv 2^2 \equiv 4\ (mod\ 8) \\ 10^1 \equiv 2\ (mod\ 8) \\ 10^0 \equiv 1\ (mod\ 8) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.18 – Valores obtidos através de restos positivos e negativos da congruência modulo 8 do número 34586.

(I)	3	4	-3	0	-2	(V) TOTAL
(II)	0	0	4	2	1	
(III) Produto	3x0=0	4x0=0	(-3)x4=-12	0x2=0	(-2)x1=-2	
(IV) Resto	0	0	-4	0	-2	-6

Fonte: Autor

Logo, teremos:

$$34586 \equiv -6 \equiv 2\ (mod\ 8)$$

Portanto, o número 34586 não é divisível por 8, pois deixa resto 2.

4.12 DIVISIBILIDADE POR 9

Exemplo 4.15. Verificar se o número 705 é divisível por 9.

Solução

A divisão pode ser definida como:

$$705 \equiv \_\ (mod\ 9)$$

Sendo $705 = 7 \cdot 10^2 + 0 \cdot 10^1 + 5 \cdot 10^0$, temos:

$$7 \cdot 10^2 + 0 \cdot 10^1 + 5 \cdot 10^0 \equiv \_\ (mod\ 9)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 7 \equiv 7\ (mod\ 9) \\ 0 \equiv 0\ (mod\ 9) \\ 5 \equiv 5\ (mod\ 9) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^2 \equiv 1^2 \equiv 1\ (mod\ 9) \\ 10^1 \equiv 1\ (mod\ 9) \\ 10^0 \equiv 1\ (mod\ 9) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.19 – Valores obtidos através da congruência modulo 9 do número 705.

(I)	7	0	5	(V) TOTAL
(II)	1	1	1	
(III) Produto	7x1=7	0x1=0	5x1=5	
(IV) Resto	7	0	5	12

Fonte: Autor

Logo, teremos:

$$705 \equiv 12 \equiv 3\ (mod\ 9)$$

Portanto, o número 705 não é divisível por 9, pois deixa resto 3.

Exemplo 4.16. Verificar se o número 605124 é divisível por 9.

Solução

A divisão pode ser definida como:

$$605124 \equiv \_\ (mod\ 9)$$

Sendo $605124 = 6 \cdot 10^5 + 0 \cdot 10^4 + 5 \cdot 10^3 + 1 \cdot 10^2 + 2 \cdot 10^1 + 4 \cdot 10^0$, temos:

$$6 \cdot 10^5 + 0 \cdot 10^4 + 5 \cdot 10^3 + 1 \cdot 10^2 + 2 \cdot 10^1 + 4 \cdot 10^0 \equiv \_\ (mod\ 9)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 6 \equiv 6\ (mod\ 9) \\ 0 \equiv 0\ (mod\ 9) \\ 5 \equiv 5\ (mod\ 9) \\ 1 \equiv 1\ (mod\ 9) \\ 2 \equiv 2\ (mod\ 9) \\ 4 \equiv 4\ (mod\ 9) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^5 \equiv 1^5 \equiv 1\ (mod\ 9) \\ 10^4 \equiv 1^4 \equiv 1\ (mod\ 9) \\ 10^3 \equiv 1^3 \equiv 1\ (mod\ 9) \\ 10^2 \equiv 1^2 \equiv 1\ (mod\ 9) \\ 10^1 \equiv 1\ (mod\ 9) \\ 10^0 \equiv 1\ (mod\ 9) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.20 – Valores obtidos através da congruência modulo 9 do número 605124.

(I)	6	0	5	1	2	4	(V) TOTAL
(II)	1	1	1	1	1	1	
(III) Produto	6x1=6	0x1=0	5x1=5	1x1=1	2x1=2	4x1=4	
(IV) Resto	6	0	5	1	2	4	18

Fonte: Autor

Logo, teremos:

$$605124 \equiv 18 \equiv 0\ (mod\ 9)$$

Portanto, o número 605124 é divisível por 9, pois deixa resto 0.

4.13 OUTRA SOLUÇÃO UTILIZANDO RESTO NEGATIVO

A divisão pode ser definida como:

$$605124 \equiv \_\ (mod\ 9)$$

Sendo $605124 = 6 \cdot 10^5 + 0 \cdot 10^4 + 5 \cdot 10^3 + 1 \cdot 10^2 + 2 \cdot 10^1 + 4 \cdot 10^0$, temos:

$$6 \cdot 10^5 + 0 \cdot 10^4 + 5 \cdot 10^3 + 1 \cdot 10^2 + 2 \cdot 10^1 + 4 \cdot 10^0 \equiv \_\ (mod\ 9)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 6 \equiv -3\ (mod\ 9) \\ 0 \equiv 0\ (mod\ 9) \\ 5 \equiv -4\ (mod\ 9) \\ 1 \equiv 1\ (mod\ 9) \\ 2 \equiv 2\ (mod\ 9) \\ 4 \equiv 4\ (mod\ 9) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^5 \equiv 1^5 \equiv 1\ (mod\ 9) \\ 10^4 \equiv 1^4 \equiv 1\ (mod\ 9) \\ 10^3 \equiv 1^3 \equiv 1\ (mod\ 9) \\ 10^2 \equiv 1^2 \equiv 1\ (mod\ 9) \\ 10^1 \equiv 1\ (mod\ 9) \\ 10^0 \equiv 1\ (mod\ 9) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.21 – Valores obtidos através de restos positivos e negativos da congruência modulo 9 do número 605124.

(I)	-3	0	-4	1	2	4	(V) TOTAL
(II)	1	1	1	1	1	1	
(III) Produto	(-3)x1= -3	0x1=0	(-4)x1= -4	1x1=1	2x1=2	4x1=4	
(IV) Resto	-3	0	-4	1	2	4	0

Fonte: Autor

Logo, teremos:

$$605124 \equiv 0\ (mod\ 9)$$

Portanto, o número 605124 é divisível por 9, pois deixa resto 0.

4.14 DIVISIBILIDADE POR 10

Exemplo 4.17. Verificar se o número 507 é divisível por 10.

Solução

A divisão pode ser definida como:

$$507 \equiv \_\ (mod\ 10)$$

Sendo $507 = 5 \cdot 10^2 + 0 \cdot 10^1 + 7 \cdot 10^0$, temos:

$$5 \cdot 10^2 + 0 \cdot 10^1 + 7 \cdot 10^0 \equiv \_\ (mod\ 10)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 5 \equiv 5\ (mod\ 10) \\ 0 \equiv 0\ (mod\ 10) \\ 7 \equiv 7\ (mod\ 10) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^2 \equiv 0^2 \equiv 0\ (mod\ 10) \\ 10^1 \equiv 0\ (mod\ 10) \\ 10^0 \equiv 1\ (mod\ 10) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.22 – Valores obtidos através da congruência modulo 10 do número 507.

(I)	5	0	7	(V) TOTAL
(II)	0	0	1	
(III) Produto	5x0=0	0x0=0	7x1=7	
(IV) Resto	0	0	7	7

Fonte: Autor

Logo, teremos:

$$507 \equiv 7\ (mod\ 10)$$

Portanto, o número 507 não é divisível por 10, pois deixa resto 7.

4.15 DIVISIBILIDADE POR 11

Exemplo 4.18. Verificar se o número 6864 é divisível por 11.

Solução

A divisão pode ser definida como:

$$6864 \equiv \_\ (mod\ 11)$$

Sendo $6864 = 6 \cdot 10^3 + 8 \cdot 10^2 + 6 \cdot 10^1 + 4 \cdot 10^0$, temos:

$$6 \cdot 10^3 + 8 \cdot 10^2 + 6 \cdot 10^1 + 4 \cdot 10^0 \equiv \_\ (mod\ 11)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 6 \equiv 6\ (mod\ 11) \\ 8 \equiv 8\ (mod\ 11) \\ 6 \equiv 6\ (mod\ 11) \\ 4 \equiv 4\ (mod\ 11) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^3 \equiv 10^2 \cdot 10 \equiv 1 \cdot 10 \equiv 10\ (mod\ 11) \\ 10^2 \equiv 100 \equiv 1\ (mod\ 11) \\ 10^1 \equiv 10\ (mod\ 11) \\ 10^0 \equiv 1\ (mod\ 11) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.23 – Valores obtidos através da congruência modulo 11 do número 6864.

(I)	6	8	6	4	(V) TOTAL
(II)	10	1	10	1	
(III) Produto	6x10=60	8x1=8	6x10=60	4x1=4	
(IV) Resto	5	8	5	4	22

Fonte: Autor

Logo, teremos:

$$6864 \equiv 22 \equiv 0\ (mod\ 11)$$

Portanto, o número 6864 é divisível por 11, pois deixa resto 0.

4.16 OUTRA SOLUÇÃO UTILIZANDO RESTO NEGATIVO

A divisão pode ser definida como:

$$6864 \equiv \_\ (mod\ 11)$$

Sendo $6864 = 6 \cdot 10^3 + 8 \cdot 10^2 + 6 \cdot 10^1 + 4 \cdot 10^0$, temos:

$$6 \cdot 10^3 + 8 \cdot 10^2 + 6 \cdot 10^1 + 4 \cdot 10^0 \equiv \_\ (mod\ 11)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 6 \equiv -5\ (mod\ 11) \\ 8 \equiv -3\ (mod\ 11) \\ 6 \equiv -5\ (mod\ 11) \\ 4 \equiv 4\ (mod\ 11) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^3 \equiv 10^2 \cdot 10 \equiv 1 \cdot (-1) \equiv -1\ (mod\ 11) \\ 10^2 \equiv (-1)^2 \equiv 1\ (mod\ 11) \\ 10^1 \equiv -1\ (mod\ 11) \\ 10^0 \equiv 1\ (mod\ 11) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.24 – Valores obtidos através de restos positivos e negativos da congruência modulo 11 do número 6864.

(I)	-5	-3	-5	4	(V) TOTAL
(II)	-1	1	-1	1	
(III) Produto	(-5)x(-1)=5	(-3)x1=-3	(-5)x(-1)=5	4x1=4	
(IV) Resto	5	-3	5	4	11

Fonte: Autor

Logo, teremos:

$$6864 \equiv 11 \equiv 0\ (mod\ 11)$$

Portanto, o número 6864 é divisível por 11, pois deixa resto 0.

2) **Observação:**

É interessante aplicar o processo de divisibilidade por congruência utilizando resto negativo para divisões em que o divisor é um valor maior 10. Pois possibilita a obtenção do resultado de uma maneira mais simples.

4.17 DIVISIBILIDADE POR 12

Exemplo 4.19. Verificar se o número 812 é divisível por 12.

Solução

A divisão pode ser definida como:

$$812 \equiv \_\ (mod\ 12)$$

Sendo $812 = 8 \cdot 10^2 + 1 \cdot 10^1 + 2 \cdot 10^0$, temos:

$$8 \cdot 10^2 + 1 \cdot 10^1 + 2 \cdot 10^0 \equiv \_\ (mod\ 12)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 8 \equiv -4\ (mod\ 12) \\ 1 \equiv 1\ (mod\ 12) \\ 2 \equiv 2\ (mod\ 12) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^2 \equiv (-2)^2 \equiv 4\ (mod\ 12) \\ 10^1 \equiv -2\ (mod\ 12) \\ 10^0 \equiv 1\ (mod\ 12) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.25 – Valores obtidos através da congruência modulo 12 do número 812.

(I)	-4	1	2	(V) TOTAL
(II)	4	-2	1	
(III) Produto	(-4)x4=-16	1x(-2)=-2	2x1=2	
(IV) Resto	-4	-2	2	-4

Fonte: Autor

Logo, teremos:

$$812 \equiv -4 \equiv 8\ (mod\ 12)$$

Portanto, o número 812 não é divisível por 12, pois deixa resto 8.

4.18 DIVISIBILIDADE POR 17

Exemplo 4.20. Verificar se o número 9435 é divisível por 17.

Solução

A divisão pode ser definida como:

$$9435 \equiv \_\ (mod\ 17)$$

Sendo $9435 = 9 \cdot 10^3 + 4 \cdot 10^2 + 3 \cdot 10^1 + 5 \cdot 10^0$, temos:

$$9 \cdot 10^3 + 4 \cdot 10^2 + 3 \cdot 10^1 + 5 \cdot 10^0 \equiv \_\ (mod\ 17)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 9 \equiv -8\ (mod\ 17) \\ 4 \equiv 4\ (mod\ 17) \\ 3 \equiv 3\ (mod\ 17) \\ 5 \equiv 5\ (mod\ 17) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^3 \equiv (-7)^2 \cdot (-7) \equiv (-2) \cdot (-7) \equiv 14 \equiv -3\ (mod\ 17) \\ 10^2 \equiv (-7)^2 \equiv 49 \equiv 15 \equiv -2\ (mod\ 17) \\ 10^1 \equiv -7\ (mod\ 17) \\ 10^0 \equiv 1\ (mod\ 17) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.26 – Valores obtidos através da congruência modulo 17 do número 9435.

(I)	-8	4	3	5	(V) TOTAL
(II)	-3	-2	-7	1	
(III) Produto	(-8)x(-3)=24	4x(-2)=-8	3x(-7)=-21	5x1=5	
(IV) Resto	7	-8	-4	5	0

Fonte: Autor

Logo, teremos:

$$9435 \equiv 0\ (mod\ 17)$$

Portanto, o número 9435 é divisível por 17, pois deixa resto 0.

4.19 DIVISIBILIDADE POR 23

Exemplo 4.21. Verificar se o número 60492 é divisível por 23.

Solução

A divisão pode ser definida como:

$$60492 \equiv \_\ (mod\ 23)$$

Sendo $60492 = 6 \cdot 10^4 + 0 \cdot 10^3 + 4 \cdot 10^2 + 9 \cdot 10^1 + 2 \cdot 10^0$, temos:

$$6 \cdot 10^4 + 0 \cdot 10^3 + 4 \cdot 10^2 + 9 \cdot 10^1 + 2 \cdot 10^0 \equiv \_\ (mod\ 23)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 6 \equiv 6\ (mod\ 23) \\ 0 \equiv 0\ (mod\ 23) \\ 4 \equiv 4\ (mod\ 23) \\ 9 \equiv 9\ (mod\ 23) \\ 2 \equiv 2\ (mod\ 23) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^4 \equiv 10^2 \cdot 10^2 \equiv 8 \cdot 8 \equiv 64 \equiv 18 \equiv -5 \ (mod\ 23) \\ 10^3 \equiv 10^2 \cdot 10 \equiv 8 \cdot 10 \equiv 80 \equiv 11 \ (mod\ 23) \\ 10^2 \equiv 100 \equiv 8 \ (mod\ 23) \\ 10^1 \equiv 10 \ (mod\ 23) \\ 10^0 \equiv 1 \ (mod\ 23) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.27 – Valores obtidos através da congruência modulo 23 do número 60492.

(I)	6	0	4	9	2	(V) TOTAL
(II)	-5	11	8	10	1	
(III) Produto	6x(-5)=-30	0x11=0	4x8=32	9x10=90	2x1=2	
(IV) Resto	-7	0	9	21	2	25

Fonte: Autor

Logo, teremos:

$$60492 \equiv 25 \equiv 2 \ (mod\ 23)$$

Portanto, o número 60492 não é divisível por 23, pois deixa resto 2.

4.18 DIVISIBILIDADE POR 36

Exemplo 4.22. Verificar se o número 576 é divisível por 36.

Solução

A divisão pode ser definida como:

$$576 \equiv \_ \ (mod\ 36)$$

Sendo $576 = 5 \cdot 10^2 + 7 \cdot 10^1 + 6 \cdot 10^0$, temos:

$$5 \cdot 10^2 + 7 \cdot 10^1 + 6 \cdot 10^0 \equiv \_ \ (mod\ 36)$$

Aplicando o Teorema 3.1 item 1, obtemos:

$$\left.\begin{array}{l} 5 \equiv 5\ (mod\ 36) \\ 7 \equiv 7\ (mod\ 36) \\ 6 \equiv 6\ (mod\ 36) \end{array}\right\} \quad (I)$$

Aplicando a Proposição 3.3, segue:

$$\left.\begin{array}{l} 10^2 \equiv 100 \equiv 28 \equiv -8\ (mod\ 36) \\ 10^1 \equiv 10\ (mod\ 36) \\ 10^0 \equiv 1\ (mod\ 36) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Tabela 4.28 – Valores obtidos através da congruência modulo 36 do número 576.

(I)	5	7	6	(V) TOTAL
(II)	-8	10	1	
(III) Produto	5x(-8)=-40	7x10=70	6x1=6	
(IV) Resto	-4	34	6	36

Fonte: Autor

Logo, teremos:

$$576 \equiv 36 \equiv 0\ (mod\ 36)$$

Portanto, o número 576 é divisível por 36, pois deixa resto 0.

5 PROPOSTA DE ENSINO

Neste capítulo será apresentada uma proposta de ensino direcionada para resoluções situações problemas envolvendo divisibilidade. O recurso utilizado para obter as soluções será o de congruência através do **algoritmo da divisibilidade por congruências (ADCG)**.

5.1 JUSTIFICATIVA

A disciplina de matemática é considerado por muitos a mais difícil de ser compreendida, visto que, a maior parte das reprovações e notas baixas está direcionada para essa área de conhecimento.

> As dificuldades de aprendizagem na Matemática podem acarretar baixos rendimentos e geram preocupações entre os envolvidos O insucesso de muitos estudantes é um fator que os leva, cada vez mais, a terem certa aversão a essa disciplina, desenvolvendo dificuldades ainda maiores com o passar dos anos escolares (Pacheco & Andreis, 2018).

A principal dificuldade apresentada pelos alunos, do ensino fundamental, é a falta de domínio em efetuar cálculos com as quatro operações básicas que são a adição, subtração, multiplicação e divisão. Esta última, em especial, é que mais compromete a aprendizagem pois apenas uma pequena quantidade é que consegue compreender como se desenvolve o processo de divisibilidade.

> Percebe-se a forma mecânica em que os alunos fazem a operação da divisão, os alunos utilizam sem compreender cada etapa que realizam no momento de efetuar a operação, e ao chegar ao resultado da divisão, não conseguem analisar se o mesmo está coerente com os dados utilizados no cálculo, e com o resultado esperado (Sales, 2013) .

A não compreensão em realizar cálculos de divisão, compromete a aprendizagem dos anos seguintes, visto que, em muitos conteúdos estudados durante todo ensino fundamental e médio se faz necessário a aplicação regras que envolvam divisibilidade.

Pensando nessa dificuldade é que se propõe apresentar neste trabalho uma possibilidade de efetuar cálculos de divisibilidade utilizando o conhecimento de congruência.

5.2 OBJETIVO GERAL

Fazer com que o aluno reflita, discuta, compreenda e aplique o conhecimento de divisibilidade em situações.

5.3 OBJETIVOS ESPECÍFICOS

- Conhecer o significado da divisão: repartição e comparação entre quantidades.
- Entender como se define uma divisão e elementos que fazem parte deste processo: dividendo, divisor, quociente e resto.
- Entender a definição de congruência.
- Conhecer as propriedades de congruência.
- Aplicar o algoritmo (ADCG) em situações que envolvam divisibilidade.

5.4 METODOLOGIA

O aprendizado de divisibilidade será através de aulas expositivas com abordagem através de exemplos.

Será apresentado ao aluno a definição do algoritmo de divisão de Euclides em que o dividendo pode ser escrito como uma multiplicação do divisor com o quociente mais o resto.

A definição de congruência o qual se baseia em uma relação de equivalência em que sendo dois números inteiros a e b, a é congruente a b módulo m, onde m é um número inteiro positivo, se e somente se, a diferença $a - b$ for divisível por m.

As propriedades de congruência são reflexiva, simétrica e transitiva e como é uma relação de equivalência, pode ser aplicado as operações de adição e multiplicação e uma vez estabelecida a congruência entre dois números inteiros. Essa

relação se mantem para qualquer valor obtido a partir da potência desses inteiros elevados a uma mesmo expoente.

Explicar como se utiliza algoritmo (ADCG) para resoluções de divisibilidades. Por fim, vários exemplos para aplicabilidade do processo de divisibilidade por congruência e atividade.

5.5 ABORDAGEM DOS CONTEÚDOS

A divisão representa uma das quatro operações fundamentais da aritmética. Este processo ocorre através do ato de dividir, ou separar, uma determinada quantidade em partes iguais.

O número que está sendo dividido em partes iguais é denominado dividendo e o número que indica em quantas vezes dividir é definido como divisor. Se a divisão ocorrer de maneira que não tenha sobras, esse processo é chamado de **divisão exata**. Mas se houver sobras, tem-se uma **divisão não exata.**

A definição deste conceito está descrita no teorema 2.1 e teve como base os exemplos 2.1 e 2.4.

Algoritmo da divisão

Dados dois números inteiros a e b, com $b \neq 0$. Existem q e r inteiros únicos tais que $a = bxq + r$, com $0 \leq r < |b|$.

Exemplo. Calcular o quociente e resto da divisão de 60 por 5.

Solução

Efetuando a divisão temos:

$$\begin{array}{r|l} 60 & 5 \\ \cline{2-2} -0- & 12 \end{array}$$

Assim**:** 60 = 5 x 12 + 0

Logo, o quociente da divisão de 60 por 5 é 12 e o resto é 0.

Exemplo. Calcular o quociente e resto da divisão de 32 por 5.

Solução

Efetuando a divisão temos:

$$\begin{array}{r|l} 32 & 5 \\ \hline -2- & 6 \end{array}$$

Assim**:** 60 = 5 x 12 + 0

Logo, o quociente da divisão de 32 por 5 é 6 e o resto é 2.

A definição deste conceito está descrita na definição 3.1, proposição 3.1 e teve como base os exemplos 3.1 e 3.2.

Congruência modulo m

Sejam a, b *e* m inteiros dados, sendo $m > 1$, dizemos que a é congruente *a* b, modulo m, denotamos $a \equiv b\ (mod\ m)$, se $m|(a - b)$. Se $m \nmid (a - b)$ dizemos que a é incongruente a b modulo m e denotamos $a \not\equiv b\ (modulo\ m)$.

Exemplo.

- $21 \equiv 15\ (mod\ 6)$, pois $6|(21 - 15)$. Observa-se que o resto da divisão dos dois números por 6 é igual a 3.
- $23 \not\equiv 32\ (mod\ 5)$, pois $5 \nmid (23 - 32)$. Logo temos que $5 \nmid -9$ e observa-se que o número 23 deixa resto 3 e o número 32 deixa resto 2 quando divididos por 5.

Se a *e* b *são inteiros, temos que* $a \equiv b\ (mod\ m)$ *se, e somente se, existir um inteiro* k *tal que* $a = b + km$.

Exemplo**.**

Se $43 \equiv 28\ (mod\ 5)$, então $5|(43 - 28)$ o que implica em $43 - 28 = 15$, isto é, $43 = 28 + 3 \cdot 5$.

A definição destas propriedades está descrita na proposição 3.2 e teve como base o exemplo 3.3.

Propriedades

Se a, b, m e d *são inteiros,* $m > 0$*, as seguintes sentenças são verdadeiras:*

1. $a \equiv a\ (mod\ m)$ (reflexiva)
2. Se $a \equiv b\ (mod\ m)$, então $b \equiv a\ (mod\ m)$ (simétrica)
3. Se $a \equiv b\ (mod\ m)$ e $b \equiv c\ (mod\ m)$, então $a \equiv c\ (mod\ m)$ (transitiva).

Exemplo.

a) Se $5|0$, então $5|(7-7)$. Logo $7 \equiv 7\ (mod\ 5)$;
b) Se $29 \equiv 5\ (mod\ 8)$, então tem-se que $29 = 5 + (3)8$. Logo, escrevendo $5 = 29 + (-3) \cdot 8$, com $-3 \in \mathbb{Z}$, obtém-se $5 \equiv 29\ (mod\ 8)$;
c) Se $31 \equiv 3\ (mod\ 7)$ e $3 \equiv 66\ (mod\ 7)$, então têm-se que $31 - 3 = (4)7\ (I)$ e $3 - 66 = (-9)7\ (II)$. Somando (I) e (II) obtém-se $31 - 66 = \big(4 + (-9)\big)7 = (-5)7$ o que implica em $31 \equiv 66\ (mod\ 7)$.

A definição destas operações em congruência está descrita no teorema 3.1 e teve como base o exemplo 3.4.

Operações com adição, subtração e multiplicação

Se a, b, c e m são inteiros tais que $a \equiv b\ (mod\ m)$, então:

1. $a + c \equiv b + c\ (mod\ m)$
2. $a - c \equiv b - c\ (mod\ m)$
3. $a \cdot c \equiv b \cdot c\ (mod\ m)$

Exemplo.

a) Se $36 \equiv 12\ (mod\ 8)$, então $36 - 12 = 3.8$. Como $36 - 12 = (36 + 10) - (12 + 10)$ temos $36 + 10 \equiv 12 + 10\ (mod\ 8)$.
b) Se $(49 - 6) - (28 - 6) = 49 - 28$ e $49 - 28 = 21 = 3 \cdot 7$, então temos que $(49 - 6) \equiv (28 - 6)(mod\ 7)$.
c) Se $54 - 34 = 2 \cdot 10$, então $54 \cdot 8 - 34 \cdot 8 = 8 \cdot 2 \cdot 10$ o que implica que $10|(54 \cdot 8 - 34 \cdot 8)$ e, portanto $54 \cdot 8 \equiv 34 \cdot 8\ (mod\ 10)$

A definição deste conceito está descrita na proposição 3.3 e teve como base o exemplo 3.5.

Potência

Se a, b, k e m são inteiros com $k > 0$ e $a \equiv b\ (mod\ m)$, então $a^k \equiv b^k\ (mod\ m)$.

Exemplo. Calcular o resto da divisão 2^{50} por 7.

Solução

Como $2^3 \equiv 8\ (mod\ 7)$ e $8 \equiv 1\ (mod\ 7)$, segue que:

$$2^{48} \equiv (2^3)^{16} \equiv 8^{16} \equiv 1^{16} \equiv 1\ (mod\ 7)$$

Assim, temos que

$$2^{48} \equiv 1\ (mod\ 7) \qquad \text{(I)}.$$

Aplicando a operação de multiplicação em (I), obtemos:

$$2^2 \cdot 2^{48} \equiv 2^2 \cdot 1\ (mod\ 7)$$

$$2^{50} \equiv 4\ (mod\ 7)$$

Logo, $2^{50} \equiv 4\ (mod\ 7)$, ou seja, a divisão de 2^{50} por 7 deixa resto 4.

Algoritmo da divisibilidade por congruências (ADCG):

Dado os números naturais D e d, para analisar se d divide D, se constrói uma matriz, seguindo o seguinte procedimento:

i) Decompomos D na forma:

$$D = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$$

ii) Calculamos para cada elemento a_i os restos na congruência módulo d

$$a_i \equiv r_i\ \ (mod\ d), \quad i = 1, \cdots, n \qquad (I)$$

Os restos r_i são colocados na primeira linha da matriz

iii) Calculamos para cada elemento b_i os restos na congruência módulo d

$$b_i \equiv s_i\ \ (mod\ d), \quad i = 1, \cdots, n \qquad (II)$$

Os restos s_i são colocados na segunda linha da matriz

iv) Como

$$a_i b_i \equiv r_i\, s_i\ \ (mod\ d), \quad i = 1, \cdots, n \qquad (III)$$

A terceira linha é formada pelo produto dos elementos da mesma coluna das linhas 1 e 2.

v) Como

$$r_i\, s_i \equiv z_i\ \ (mod\ d), \quad i = 1, \cdots, n \qquad (IV)$$

A quarta linha é formada pelos restos obtidos a partir resultado do produto da terceira linha.

vi) Como

$$D = a_1b_1 + \cdots + a_{nb_n} \equiv r_1\, s_1 + \cdots r_n s_n \equiv z_1 + \cdots z_n \ (mod\ d), \qquad (V)$$

Esta soma dos restos é colocada na última coluna da matriz. Se for necessário se faz uma última equivalência para que a soma seja menor que d.

vii) Se o resto em $V)$ é zero concluímos que d divide D, caso contrário d não divide D.

viii) A matriz toma a seguinte forma:

Valores obtidos através da congruência modulo d do número D.

(I)	r_1	r_2	...	r_n	(V) TOTAL
(II)	s_1	s_2	...	s_n	
(III) Produto	r_1s_1	r_2s_2	...	r_ns_n	
(IV) Resto	z_1	z_2	...	z_n	z_1+ ...+z_n

Fonte: Autor

Para desenvolver este conceito foi utilizado como base os exemplos 4.1, 4.4, 4.5, 4.10 e 4.18.

Divisibilidade por 2

Exemplo. Verificar se o número 4637 é divisível por 2.

Solução: A divisão pode ser definida como:

$$4637 \equiv \_\ (mod\ 2)$$

Sendo $4637 = 4 \cdot 10^3 + 6 \cdot 10^2 + 3 \cdot 10^1 + 7 \cdot 10^0$, temos:

$$4 \cdot 10^3 + 6 \cdot 10^2 + 3 \cdot 10^1 + 7 \cdot 10^0 \equiv \_\ (mod\ 2)$$

Aplicando a congruência em cada um dos coeficientes, obtemos:

$$\left.\begin{array}{l} 4 \equiv 0\ (mod\ 2) \\ 6 \equiv 0\ (mod\ 2) \\ 3 \equiv 1\ (mod\ 2) \\ 7 \equiv 1\ (mod\ 2) \end{array}\right\} \quad (I)$$

Aplicando a congruência nas potências de base 10, segue:

$$\left.\begin{array}{l} 10^3 \equiv 0^3 \equiv 0\ (mod\ 2) \\ 10^2 \equiv 0^2 \equiv 0\ (mod\ 2) \\ 10^1 \equiv 0\ (mod\ 2) \\ 10^0 \equiv 1\ (mod\ 2) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Valores obtidos através da congruência modulo 2 do número 4637.

(I)	0	0	1	1	(V) TOTAL
(II)	0	0	0	1	
(III) Produto	0x0 = 0	0x0 = 0	1x0 = 0	1x1 = 1	
(IV) Resto	0	0	0	1	1

Fonte: Autor

Logo, teremos:

$$4637 \equiv 1\ (mod\ 2)$$

Portanto, o número 4637 não é divisível por 2, pois deixa resto 1.

Divisibilidade por 3

Exemplo. Verificar se o número 732 é divisível por 3.

Solução: A divisão pode ser definida como:

$$732 \equiv \_\ (mod\ 3)$$

Sendo $732 = 7 \cdot 10^2 + 3 \cdot 10^1 + 2 \cdot 10^0$, temos:

$$7.10^2 + 3.10^1 + 2.10^0 \equiv \_\ (mod\ 3)$$

Aplicando a congruência em cada um dos coeficientes, obtemos:

$$\left.\begin{array}{l} 7 \equiv 1\ (mod\ 3) \\ 3 \equiv 0\ (mod\ 3) \\ 2 \equiv 2\ (mod\ 3) \end{array}\right\} \quad (I)$$

Aplicando a congruência nas potências de base 10, segue:

$$\left.\begin{array}{l} 10^2 \equiv 1^2 \equiv 1\ (mod\ 3) \\ 10^1 \equiv 1\ (mod\ 3) \\ 10^0 \equiv 1\ (mod\ 3) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Valores obtidos através da congruência modulo 3 do número 732.

(I)	1	0	2	(V) TOTAL
(II)	1	1	1	
(III) Produto	1x1 = 1	0x1 = 0	2x1 = 2	
(IV) Resto	1	0	2	3

Fonte: Autor

Logo, teremos:

$$732 \equiv 3 \equiv 0\ (mod\ 3)$$

Portanto, o número 732 é divisível por 3, pois deixa resto 0.

Divisibilidade por 4

Exemplo**.** Verificar se o número 5763 é divisível por 4.

Solução: A divisão pode ser definida como:

$$5763 \equiv \_\ (mod\ 4)$$

Sendo $5763 = 5 \cdot 10^3 + 7 \cdot 10^2 + 6 \cdot 10^1 + 3 \cdot 10^0$, temos:

$$5 \cdot 10^3 + 7 \cdot 10^2 + 6 \cdot 10^1 + 3 \cdot 10^0 \equiv \_\ (mod\ 4)$$

Aplicando a congruência em cada um dos coeficientes, obtemos:

$$\left.\begin{array}{l} 5 \equiv 1\ (mod\ 4) \\ 7 \equiv 3\ (mod\ 4) \\ 6 \equiv 2\ (mod\ 4) \\ 3 \equiv 3\ (mod\ 4) \end{array}\right\} \quad (I)$$

Aplicando a congruência nas potências de base 10, segue:

$$\left.\begin{array}{l} 10^3 \equiv 2^3 \equiv 2^2 \cdot 2 \equiv 0 \cdot 2 \equiv 0\ (mod\ 4) \\ 10^2 \equiv 2^2 \equiv 0\ (mod\ 4) \\ 10^1 \equiv 2\ (mod\ 4) \\ 10^0 \equiv 1\ (mod\ 4) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Valores obtidos através da congruência modulo 4 do número 5763.

(I)	1	3	2	3	(V) TOTAL
(II)	0	0	2	1	
(III) Produto	1x0 = 0	3x0 = 0	2x2 = 4	3x1 = 3	
(IV) Resto	0	0	4	3	7

Fonte: Autor

Logo, teremos:

$$5763 \equiv 7 \equiv 3\ (mod\ 4)$$

Portanto, o número 5763 não é divisível por 4, pois deixa resto 3.

Divisibilidade por 6

Exemplo. Verificar se o número 9347 é divisível por 6.

Solução: A divisão pode ser definida como:

$$9347 \equiv \_\ (mod\ 6)$$

Sendo $9347 = 9 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10^1 + 7 \cdot 10^0$, temos:

$$9 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10^1 + 7 \cdot 10^0 \equiv \_\ (mod\ 6)$$

Aplicando a congruência em cada um dos coeficientes, obtemos:

$$\left.\begin{array}{l} 9 \equiv 3\ (mod\ 6) \\ 3 \equiv 3\ (mod\ 6) \\ 4 \equiv 4\ (mod\ 6) \\ 7 \equiv 1\ (mod\ 6) \end{array}\right\} \quad (I)$$

Aplicando a congruência nas potências de base 10, segue:

$$\left.\begin{array}{l} 10^3 \equiv 4^3 \equiv 4^2 \cdot 4 \equiv 4 \cdot 4 \equiv 16 \equiv 4\ (mod\ 6) \\ 10^2 \equiv 4^2 \equiv 16 \equiv 4\ (mod\ 6) \\ 10^1 \equiv 4\ (mod\ 6) \\ 10^0 \equiv 1\ (mod\ 6) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Valores obtidos através da congruência modulo 6 do número 9347.

(I)	3	3	4	1	(V) TOTAL
(II)	4	4	4	1	
(III) Produto	3x4 = 12	3x4 = 12	4x4 = 16	1x1 = 1	
(IV) Resto	0	0	4	1	5

Fonte: Autor

Logo, teremos:

$$9347 \equiv 5\ (mod\ 6)$$

Portanto, o número 9347 não é divisível por 6, pois deixa resto 5.

Outra solução utilizando resto negativo

Solução: A divisão pode ser definida como:

$$9347 \equiv \_\ (mod\ 6)$$

Sendo $9347 = 9 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10^1 + 7 \cdot 10^0$, temos:

$$9.10^3 + 3.10^2 + 4.10^1 + 7.10^0 \equiv \_\ (mod\ 6)$$

Aplicando a congruência em cada um dos coeficientes, obtemos:

$$\left.\begin{array}{l} 9 \equiv 3\ (mod\ 6) \\ 3 \equiv 3\ (mod\ 6) \\ 4 \equiv -2\ (mod\ 6) \\ 7 \equiv 1\ (mod\ 6) \end{array}\right\} \quad (I)$$

Aplicando a congruência nas potências de base 10, segue:

$$\left.\begin{array}{l} 10^3 \equiv 4^3 \equiv 4^2 \cdot 4 \equiv (-2) \cdot (-2) \equiv 4 \equiv -2 \ (mod\ 6) \\ 10^2 \equiv 4^2 \equiv 16 \equiv 4 \equiv -2 \ (mod\ 6) \\ 10^1 \equiv 4 \equiv -2 \ (mod\ 6) \\ 10^0 \equiv 1 \ (mod\ 6) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Valores obtidos através de restos positivos e negativos da congruência modulo 6 do número 9347.

(I)	3	3	-2	1	(V) TOTAL
(II)	-2	-2	-2	1	
(III) Produto	3x(-2) = -6	3x(-2) = -6	(-2)x(-2) = 4	1x1 = 1	
(IV) Resto	0	0	4	1	5

Fonte: Autor

Logo, teremos:

$$9347 \equiv 5 \ (mod\ 6)$$

Portanto, o número 9347 não é divisível por 6, pois deixa resto 5.

Divisibilidade por 11

Exemplo. Verificar se o número 6864 é divisível por 11.

Solução: A divisão pode ser definida como:

$$6864 \equiv \_ \ (mod\ 11)$$

Sendo $6864 = 6 \cdot 10^3 + 8 \cdot 10^2 + 6 \cdot 10^1 + 4 \cdot 10^0$, temos:

$$6 \cdot 10^3 + 8 \cdot 10^2 + 6 \cdot 10^1 + 4 \cdot 10^0 \equiv \_ \ (mod\ 11)$$

Aplicando a congruência em cada um dos coeficientes, obtemos:

$$\left.\begin{array}{l} 6 \equiv 6 \ (mod\ 11) \\ 8 \equiv 8 \ (mod\ 11) \\ 6 \equiv 6 \ (mod\ 11) \\ 4 \equiv 4 \ (mod\ 11) \end{array}\right\} \quad (I)$$

Aplicando a congruência nas potências de base 10, segue:

$$\left.\begin{array}{l} 10^3 \equiv 10^2 \cdot 10 \equiv 1 \cdot 10 \equiv 10\ (mod\ 11) \\ 10^2 \equiv 100 \equiv 1\ (mod\ 11) \\ 10^1 \equiv 10\ (mod\ 11) \\ 10^0 \equiv 1\ (mod\ 11) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Valores obtidos através da congruência modulo 11 do número 6864.

(I)	6	8	6	4	(V) TOTAL
(II)	10	1	10	1	
(III) Produto	6x10=60	8x1=8	6x10=60	4x1=4	
(IV) Resto	5	8	5	4	22

Fonte: Autor

Logo, teremos:

$$6864 \equiv 22 \equiv 0\ (mod\ 11)$$

Portanto, o número 6864 é divisível por 11, pois deixa resto 0.

Outra solução utilizando restos negativos

A divisão pode ser definida como:

$$6864 \equiv \_\_\ (mod\ 11)$$

Sendo $6864 = 6 \cdot 10^3 + 8 \cdot 10^2 + 6 \cdot 10^1 + 4 \cdot 10^0$, temos:

$$6 \cdot 10^3 + 8 \cdot 10^2 + 6 \cdot 10^1 + 4 \cdot 10^0 \equiv \_\_\ (mod\ 11)$$

Aplicando a congruência em cada um dos coeficientes, obtemos:

$$\left.\begin{array}{l} 6 \equiv -5\ (mod\ 11) \\ 8 \equiv -3\ (mod\ 11) \\ 6 \equiv -5\ (mod\ 11) \\ 4 \equiv 4\ (mod\ 11) \end{array}\right\} \quad (I)$$

Aplicando a congruência nas potências de base 10, segue:

$$\left.\begin{array}{l} 10^3 \equiv 10^2 \cdot 10 \equiv 1 \cdot (-1) \equiv -1\ (mod\ 11) \\ 10^2 \equiv (-1)^2 \equiv 1\ (mod\ 11) \\ 10^1 \equiv -1\ (mod\ 11) \\ 10^0 \equiv 1\ (mod\ 11) \end{array}\right\} \quad (II)$$

Aplicando o Algoritmo ADCG no exemplo, a matriz tem a seguinte forma:

Valores obtidos através de restos positivos e negativos da congruência modulo 11 do número 6864.

(I)	-5	-3	-5	4	(V) TOTAL
(II)	-1	1	-1	1	
(III) Produto	(-5)x(-1)=5	(-3)x1=-3	(-5)x(-1)=5	4x1=4	
(IV) Resto	5	-3	5	4	11

Fonte: Autor

Logo, teremos:

$$6864 \equiv 11 \equiv 0\ (mod\ 11)$$

Portanto, o número 6864 é divisível por 11, pois deixa resto 0.

Observação:

É interessante aplicar o processo de divisibilidade por congruência utilizando restos negativos para divisões em que o divisor é um valor maior 10. Pois possibilita a obtenção do resultado de uma maneira mais simples.

5.6 ATIVIDADES

Utilizando o algoritmo de divisibilidade por congruência (ADCG). Verificar se os números 632, 5194, 32079, 462081 e 38291650 são divisíveis por 5, 7, 8, 9 e 10 respectivamente.

CONSIDERAÇÕES FINAIS

O desenvolvimento deste trabalho possibilitou uma abordagem diferenciada do estudo de divisibilidade utilizando o conteúdo de congruência. Em muitos livros didáticos encontra-se apenas uma maneira de se determinar a divisibilidade de um número por outro, este procedimento inclui muitas regras que acabam dificultando o processo de aprendizagem do aluno.

A dificuldade em efetuar cálculos prejudica o desenvolvimento do conhecimento matemático, pois o estudante que não consegue realizá-los apresentará muita dificuldade para compreender e aprender conteúdos de anos posteriores, ou seja, para que o aluno tenha um aprendizado significativo se faz necessário o uso de procedimentos contidos em assuntos anteriores.

O estudo de congruência proporciona a possibilidade de calcular divisibilidades utilizando relações de equivalências. Estas, permitem obter o resto de uma divisão de uma maneira mais simples, sem ter que recorrer a regras específicas, ou seja, os procedimentos utilizados para realizar tal operação podem ser aplicados em qualquer situação independentemente de quais números que fazem parte do problema.

Desse modo, criou-se um recurso metodológico denominado Algoritmo de Divisibilidade por Congruência (ADCG) para verificar os processos de divisibilidades. O (ADCG) contribui para o aprendizado de divisões, aprimoramento do uso de congruência e possibilita despertar o interesse do aluno para o estudo de novos conhecimentos.

Este recurso certamente poderá contribuir para a melhoria na qualidade de ensino e por esse motivo é que se propôs, neste trabalho, desenvolver uma proposta de ensino com objeto de auxiliar, intensificar e melhorar o entendimento do conteúdo ministrado em sala de aula.

REFERÊNCIAS

Matemática e os números naturais. **A História dos Números Naturais**. Disponível em: <https://sites.google.com/site/matematicaeosnumerosnaturais/home/a-historia-dos-numeros-naturais>. acesso em 15 de março de 2019.

B. Boyer, Carl– **História da matemática** / Carl B. Boyer, Uta C. Merzbach; [tradução de Helena Castro]: São Paulo: Blucher,2012.

Mat. UFRGS. **História dos Números**. Disponível em: <www.mat.ufrgs.br/~vclotilde/disciplinas/html/historia_numeros.pdf>. Acesso em 20 de março de 2019.

Pacheco, M.B., & Andreis, G.d,(2018). **Causas das dificuldades de aprendizagem em matemática:** percepção de professores e estudantes no 3º ano do Ensino Médio. *Revista principia,* Disponível em: < https://www.infoescola.com/pedagogia/possibilidades-e-limitacoes-as-dificuldades-existentes-no-processo-de-ensino-aprendizagem-da-matematica>. Acesso em 21 de março de 2019.

MORGADO, Augusto c. e CARVALHO, Paulo c. Pinto – **Matemática Discreta** – Rio de Janeiro: SBM,2013.

PIANO1, Diogo Leandro; LOUREIRO1, Daniel Zampieri; LANGER, Arleni Elise Sella. História. **Técnicas e as Problemáticas do Ensino e Aprendizagem da Divisão**: XXV Semana Acadêmica Da Matemática ISSN 1981-8645.

SANTOS, Jose Plínio de Oliveira. **Introdução à Teoria Dos Números**. Rio de Janeiro: IMPA, 2006.

Pereira da silva, Luis Henrique. **Uma aplicação de congruência na determinação de critérios de divisibilidade**. [manuscrito] / Luis Henrique Pereira da silva.-2015.

SILVEIRA, Ênio. **Matemática Compreensão e Prática 6º Ano**. São Paulo, 2015. Moderna.

MARCONI, M. A.; LAKATOS, E. M. **Metodologia do trabalho científico**. 9.ed.Editora Atlas São Paulo. 2007.

BOSQUILHA, Alessandra; AMARAL, João Tomás. **Minimanual Compacto de Matématica Ensino Fundamental: Teoria e Prática**. São Paulo, 2003. Rideel.

SALES, Daisy Aparecida Rodrigues. **Os desafios da escola pública paranaense na perspectiva do professor**- Produções Didáticas-Pedagógicas. Volume II. Ano 2013. Paraná