UNIVERSIDADE FEDERAL DO MARANHÃO
Fundação Instituída nos termos da Lei 5.152 de 21/10/1966 - São Luís - MA
Centro de Ciências Exatas e Tecnologia
Curso de Matemática – Licenciatura

Glenda Gracyanne Silva de Azevedo Sousa

Determinação de critérios de divisibilidade pelo inteiro sete através de congruência: o teste de Chika Ofili

São Luís - MA
2023

Glenda Gracyanne Silva de Azevedo Sousa

Determinação de critérios de divisibilidade pelo inteiro sete através de congruência: o teste de Chika Ofili

Monografia (Trabalho de Conclusão de Curso) apresentada à Coordenadoria dos cursos de Matemática, da Universidade Federal do Maranhão, como requisito parcial para obtenção do grau de Licenciada em Matemática.

Curso de Matemática – Licenciatura

Universidade Federal do Maranhão

Orientador: Prof. Dr. Luís Fernado Coelho Amaral

São Luís - MA

2023

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Diretoria Integrada de Bibliotecas/UFMA

Sousa, Glenda Gracyanne Silva de Azevedo.
Determinação de critérios de divisibilidade pelo inteiro sete através de congruência: o teste de Chika Ofili / Glenda Gracyanne Silva de Azevedo Sousa. - 2023.
39 f.

Orientador(a): Luís Fernando Coelho Amaral.
Monografia (Graduação) - Curso de Matemática, Universidade Federal do Maranhão, São Luís, 2023.

1. Congruência. 2. Critério de divisibilidade por 7. 3. Divisibilidade por 7. I. Amaral, Luís Fernando Coelho. II. Título.

Glenda Gracyanne Silva de Azevedo Sousa

Determinação de critérios de divisibilidade pelo inteiro sete através de congruência: o teste de Chika Ofili

Monografia (Trabalho de Conclusão de Curso) apresentada à Coordenadoria dos cursos de Matemática, da Universidade Federal do Maranhão, como requisito parcial para obtenção do grau de Licenciada em Matemática.

Trabalho **APROVADO**. São Luís - MA, 22/12/2023

Prof. Dr. Luís Fernado Coelho Amaral
DEMAT/UFMA
Orientador

Prof.ª Sonia Rocha Santos Sousa
UFMA
Primeira Examinadora

Prof. Dr. Marcos Antonio Ferreira de Araújo
DEMAT/UFMA
Segundo Examinador

Dedico essa monografia ao meu filho Heitor Lucca, a motivação da minha vida.

Agradecimentos

Quero começar este importante momento de agradecimentos com uma profunda gratidão a Deus, o supremo criador de todas as coisas e o maior arquiteto dos meus sonhos. Sua orientação divina guiou cada passo desta jornada acadêmica, fortalecendo minha determinação e iluminando o meu caminho.

Ao professor Dr. Luís Fernando Coelho Amaral, desejo expressar minha sincera gratidão por ter aceitado a missão de me orientar neste trabalho. Sua dedicação, sabedoria e comprometimento com a excelência acadêmica foram fundamentais para a realização deste projeto. A orientação que recebi sob sua tutela não apenas enriqueceu meu conhecimento, mas também me inspirou a alcançar níveis mais altos de desempenho.

Quero estender meus agradecimentos calorosos aos membros da banca examinadora, cuja participação e avaliação rigorosa acrescentaram valor significativo ao meu trabalho. A contribuição de vocês enriqueceu o conteúdo desta monografia e fortaleceu a qualidade da pesquisa.

Não posso deixar de mencionar minha família, cujo apoio inabalável tem sido um pilar essencial ao longo dessa jornada acadêmica. Desde o momento em que escolhi este curso até o presente, vocês estiveram ao meu lado, oferecendo amor, incentivo e compreensão. Cada conquista alcançada é compartilhada com vocês, pois sei que o mérito também pertence a cada membro da minha família.

Por último, mas definitivamente não menos importante, quero expressar minha profunda gratidão aos meus colegas e professores da graduação. Durante todos esses anos, suas amizades e mentorias foram inestimáveis. As amizades que fiz ao longo deste percurso acadêmico não são apenas conexões, mas laços que enriqueceram minha vida e minha jornada de aprendizado.

E, é claro, não posso esquecer de estender meu agradecimento à Universidade Federal do Maranhão por tudo. Esta instituição de ensino superior desempenhou um papel fundamental em minha formação, fornecendo um ambiente propício para a exploração intelectual e o crescimento pessoal. Cada instante passado nesta universidade contribuiu para moldar minha mente e minha visão de mundo.

Em resumo, esta conquista é o resultado de um esforço conjunto e da generosidade de muitos. Espero que esta seja apenas a primeira etapa de muitas conquistas futuras.

Muito obrigado a todos!

"Cada fracasso nos ensina algo que necessitávamos aprender."

Charles Dickens (1812 – 1870)

Resumo

O presente estudo tem como desígnio principal a apresentação e análise da derivação de critérios de divisibilidade pelo número inteiro 7, com base na aplicação da congruência. Esta análise se desenvolve a partir de uma comparação entre o critério tradicional de divisibilidade por 7 que é geralmente descrito na literatura matemática e o critério proposto por Chika Ofili, em 2019. O objetivo central deste trabalho é desvendar a riqueza e complexidade subjacentes à teoria dos números, evidenciando como a congruência se manifesta como uma ferramenta poderosa na determinação de critérios de divisibilidade. Além disso, ao explorar o critério de Chika Ofili, buscamos impulsionar potenciais extensões dessa descoberta na teoria dos números. Este estudo não apenas ilumina uma área crucial da matemática mas também presta homenagem ao espírito inovador de mentes jovens que continuam a enriquecer o campo do conhecimento matemático com contribuições significativas.

Palavras-chave: Divisibilidade por 7, congruência, Chika Ofili.

Abstract

The main purpose of the present study is to present and analyze the derivation of divisibility criteria by the integer 7, based on the application of congruence. This analysis is developed from a comparison between the traditional criterion of divisibility by 7 that is generally described in the mathematical literature and the criterion proposed by Chika Ofili, in 2019. The main objective of this work is to unravel the richness and complexity underlying number theory, evidencing as the congruence is manifests itself as a powerful tool in determining divisibility criteria. In addition, by exploring Chika Ofili's criterion, we seek to boost potential extensions of this discovery in number theory. This study doesn't just shine a light on a crucial area of mathematics but also pays tribute to the innovative spirit of young minds that continue to enrich the field of mathematical knowledge with contributions Significant.

Keywords: Divisibility by 7; congruence; Chika Ofili.

Lista de ilustrações

Lista de tabelas

Sumário

Introdução

A Matemática é uma ciência fascinante pela sua ampla aplicabilidade por diversas áreas do conhecimento mas também por proporcionar a qualquer indivíduo condições que o oportunizem a realização de descobertas que venham cada vez mais agregar valor à mesma, como é o caso de Chika Ofili, um jovem nigeriano que em 2019, aos 12 anos de idade, se tornou notícia entre as comunidades de matemáticos após supostamente ter descoberto e proposto um novo método como critério de divisibilidade para o inteiro sete.

Com base na leitura de um artigo escrito pelo meu orientador e proposto à Revista do Professor de Matemática que relata este acontecimento, é que resolvi realizar o meu trabalho de conclusão de curso. Analisar a hipótese do garoto em relação aos critérios de divisibilidade por sete que encontramos disponíveis na literatura permite que reconheçamos uma relação bastante interessante que aqui será analisada e generalizada para o conjunto dos inteiros, à luz de conhecimentos básicos sobre congruência linear.

Divisibilidade é um dos temas mais básicos em Teoria dos Números e os critérios de divisibilidade, em geral, resumem-se a um conjunto de condições que permitem aferir se um inteiro a é divisível, ou não, por um outro inteiro b, tendo como base a representação decimal destes inteiros. Entretanto, entre os critérios de divisibilidade estabelecidos para os dez primeiros inteiros positivos, os critérios de divisibilidade pelo inteiro 7 são pouco inteligíveis, e isto se deve ao fato de estes critérios não diferenciarem-se de uma aplicação do habitual algoritmo da divisão.

Congruência é uma poderosa ferramenta no estudo da divisibilidade por permitir a execução de uma aritmética com os restos de uma divisão euclidiana, no caso deste trabalho pelo sete. Este trabalho se destina a mostrar como aritmética básica unida a esta noção cada vez mais fecunda em Teoria dos Números são úteis no estabelecimento de critérios de divisibilidade similares.

Compreender a aplicação de vários critérios de divisibilidade por sete por meio da congruência, em particular, a um nível superior, é um processo relativamente simples, especialmente quando se considera um critério específico, como o proposto por Chika Ofili. Essa abordagem permite explorar a lógica subjacente à congruência e como resultado, o processo de determinar a divisibilidade por sete se torna mais cativante e estimulante, desafiando nossa compreensão e incentivando a busca por entendimento em vez de depender puramente da memorização.

Este trabalho tem como objetivo apresentar o método proposto por Chika Ofili para utilizá-lo em uma eventual comparação ao critério de divisibilidade por sete encontrado

na bibliografia, objetivando exibir uma relação de congruência existente na determinação destes.

Dessa forma este trabalho visa incentivar à reflexão e a impulsão a novas descobertas principalmente por graduandos mas também qualquer pessoa que se dedique a obter conhecimentos básicos de aritmética. Desse modo esperamos apresentar um conteúdo útil e relevante, especialmente no que se refere à didática para qualquer pessoa que se interessa pela matemática.

A seguir é apresentada uma breve descrição de cada capítulo.

O capítulo 1 se dedica a expor os conceitos fundamentais para o compreendimento da proposta desse trabalho e para tanto são apresentados conteúdos e propriedades elementares de Teoria dos Números como bases, conjunto dos números inteiros, divisibilidade e máximo divisor comum. Após isso, no capítulo 2, o conceito de congruência é introduzido.

O capítulo 3 apresenta a suposta descoberta do garoto Chika Ofili além de sua demonstração. Em seguida, é apresentada uma análise entre os critérios de divisibilidade por sete proposto por Chika Ofili e o critério que é geralmente apresentado na literatura disponível. E finalmente, será exibida a determinação de critérios de divisibilidade por sete através de congruência. No último capítulo as considerações finais de trabalho são feitas.

Este trabalho se caracteriza como uma pesquisa descritiva explicativa, visando explorar e explicar o tema em questão, fornecendo informações adicionais a respeito e para tanto, emprega o método de pesquisa bibliográfica para coletar informações relacionadas ao tema por meio da análise de materiais disponíveis na literatura. Nesse contexto, utilizá-se fontes secundárias para demonstrar a relação de congruência na determinação dos critérios de divisibilidade por sete.

O tema é relevante, pouco explorado e difundido na literatura. Analisá-lo minuciosamente, além do que este trabalho se propõe, permite o engajamento para o estudo de $\mathbb{Z}_7$.

1 Introdução aos números inteiros e conceitos básicos

Neste primeiro capítulo iremos definir alguns conceitos e resultados sobre números inteiros e sobre a teoria da divisibilidade que nos serão pertinentes no desenvolvimento do trabalho. Destacamos que as notações empregadas aqui são usais e encontradas na maioria dos livros relacionados aos temas.

1.1 Números inteiros

O conjunto dos números inteiros emerge como uma construção matemática essencial, que abarca tanto os números naturais positivos quanto seus negativos, além do zero. Sua evolução está intrinsecamente ligada ao desenvolvimento da humanidade na busca por uma maneira de quantificar e descrever as quantidades, o que segundo MILIES; COELHO (1998) se deve a possibilidade de interpretá-los de diversas formas. No entanto, foi somente na Grécia antiga que formalizou-se o conjunto dos inteiros como uma entidade abstrata e independente, por meio das obras de matemáticos como Euclides, que explorou a natureza dos números primos, e de Pitágoras, que investigou as propriedades numéricas e suas relações.

1.1.1 Propriedades

Os números inteiros integram um conjunto que designaremos por $\mathbb{Z}$. Neste conjunto "estão definidas duas operações, que chamaremos de adição e multiplicação e denotaremos por $+$ e $\cdot$" (MILIES; COELHO, 1998, pág. 13), além de uma relação, denominada "menor ou igual", indicada por $\leq$, que nos permite comparar os elementos deste conjunto.

Os axiomas que apresentaremos a seguir caracterizarão propriedades fundamentais das operações e da relação de ordem do conjunto dos inteiros. De posse destes conceitos, quaisquer propriedades de $\mathbb{Z}$ podem ser deduzidas. Dados $a,\ b$ e $c \in \mathbb{Z}$, tem-se:

O primeiro grupo de axiomas expõe algumas propriedades relacionadas à soma:

Axioma 1.1. *Propriedade Associativa:* $(a + b) + c = a + (b + c)$.

Axioma 1.2. *Propriedade Comutativa:* $a + b = b + a$.

Axioma 1.3. *Existência do Elemento Neutro:* $0 + a = a$.

Axioma 1.4. *Existência do Oposto:* $a + (-a) = a - a = 0$.

Axioma 1.5. *Existe um único $x \in \mathbb{Z}$ tal que $b + x = a$, a, $b \in \mathbb{Z}$ e é denominado por $a + (-b)$, chamado diferença de a e b.*

O grupo de aximas a seguir descreve propriedades relacionadas à multiplicação:

Axioma 1.6. *Propriedade Associativa:* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Axioma 1.7. *Propriedade Comutativa:* $a \cdot b = b \cdot a$.

Axioma 1.8. *Existência do neutro:* $1 \cdot a = a$.

Axioma 1.9. *Propriedade Cancelativa: Para $a \neq 0$, tem-se que, se $a \cdot b = a \cdot c$, então $b = c$.*

O último axioma diz respeito às duas operações.

Axioma 1.10. *Propriedade Distributiva:* $a \cdot (b + c) = a \cdot b + a \cdot c$.

1.1.2 Ordenação dos Inteiros

A relação de ordem nos números inteiros é essencial para entender a divisibilidade, permitindo identificar padrões e determinar rapidamente se um número é múltiplo de outro. Ela simplifica a análise de divisores, múltiplos e números primos, tornando mais claro o estudo da divisibilidade e sua aplicação.

Enunciaremos a partir de agora, axiomas referentes ao que MILIES; COELHO (1998) denominaram como por "relação menor ou igual".

Axioma 1.11. *Propriedade reflexiva: Para todo inteiro a tem-se que $a \leq a$.*

Axioma 1.12. *Propriedade anti-simétrica: Dados dois inteiros a e b, se $a \leq b$ e $b \leq a$, então $a = b$.*

Axioma 1.13. *Propriedade transitiva: Para todos a, b e $c \in \mathbb{Z}$, se $a \leq b$ e $b \leq c$, então $a \leq c$.*

Devidos aos axiomas 1.11, 1.12 e 1.13, a *relação menor ou igual* é uma *relação de ordem* e para indicar que $a \leq b$ (quando $a \neq b$), isto é, quando *a é menor que b*, utilizaremos a simbologia $a < b$. No que se segue, utilizaremos os termos positivo e negativo em seus significados usuais, isto é, para indicar um certo número é maior ou menor que zero, respectivamente. Quando for adequado, utilizaremos os símbolos $b \geq a$ ou $b > a$ para indicar que $a \leq b$ ou $a < b$.

Axioma 1.14. *Tricotomia: Dados dois inteiros a e b tem-se que ou $a < b$ ou $a = b$ ou $b < a$.*

Temos que introduzir ainda alguns axiomas que vinculem a relação de ordem às operações:

Axioma 1.15. *Para todos a, b e $c \in \mathbb{Z}$, se $a \leq b$, então $a + c \leq b + c$.*

Axioma 1.16. *Para todos a, b e $c \in \mathbb{Z}$, se $0 \leq c$, então $a \cdot c \leq b \cdot c$.*

Para apresentarmos um último axioma, é necessário introduzirmos alguns conceitos, o que realizaremos a seguir.

Definição 1.17. *Seja A um subconjunto de $\mathbb{Z}$. Diz-se que A é limitado inferiormente se existe um $k \in \mathbb{Z}$, tal que para todo $a \in A$, tem-se que $k \leq a$.*

Um elemento $a_0 \in A$ diz-se *elemento mínimo de A* se, para todo $a \in A$, tem-se que $a_0 \leq a$. E de maneira análoga, pode-se definir um conjunto *limitado superiormente* e *elemento máximo* de um conjunto. Utilizaremos os símbolos *min A* e *max A* para indicar o mínimo e o máximo de um conjunto, quando estes existirem.

Axioma 1.18. *(Princípio da Boa Ordem): Todo conjunto não-vazio de inteiros não negativos contém elemento mínimo.*

Proposição 1.19. *Seja $a \in \mathbb{Z}$, tal que $0 \leq a \leq 1$. Então $a = 0$ ou $a = 1$.*

Demonstração: Suponhamos, por absurdo, que exista um inteiro a diferente 0 e 1, nessas condições. Assim, o conjunto $S = \{a \in \mathbb{Z} \mid 0 < a < 1\}$ seria não vazio e pelo Princípio da Boa Ordem, existiria $m = min\ S$. Como $m \in \mathbb{Z}$ temos que $m > 0$ e $m < 1$. Utilizando do Axioma 1.16, multiplicando por m a segunda igualdade, obtemos $m^2 < m$. Assim, $m^2 > 0$ e como $m < 1$, pela Axioma 1.13 temos $m^2 < 1$. Logo $m^2 \in S$ e é menor que seu elemento mínimo, uma contradição.

■

1.1.2.1 Valor absoluto de um inteiro

O conhecimento sobre valor absoluto de um número inteiro desempenha um papel crucial no estudo e na ordenação do conjunto dos números inteiros. O valor absoluto, representado pela distância do número até o zero na reta numérica, é uma ferramenta essencial que nos ajuda a compreender a relação entre os números e a estabelecer uma ordenação clara e coerente.

Definição 1.20. *Chama-se valor absoluto de um inteiro a, ao inteiro que se indica $\mid a \mid$, e é tal que:*

$$\mid a \mid = \begin{cases} a, \ se\ a \geq 0 \\ (-a), \ se\ a < 0 \end{cases}$$

Conhecer as propriedades elementares dos números inteiros, como a ordenação e o valor absoluto, é de fundamental importância para estabelecer uma base sólida de compreensão desse conjunto numérico. A ordenação dos inteiros permite a identificação de relações de magnitude entre os números, tornando possível reconhecer padrões, relações de divisibilidade e estabelecer critérios de comparação. Essa propriedade desempenha um papel crucial em campos que vão desde a teoria dos números até aplicações práticas em ciências naturais e engenharia.

Além disso, o conceito de valor absoluto proporciona uma medida objetiva da distância entre um número e zero, independente de sua posição na reta numérica. Isso não só simplifica a resolução de equações e desigualdades, mas também tem aplicações vitais em áreas como geometria e análise matemática.

1.2 Divisibilidade

A divisibilidade é um conceito fundamental na matemática por descrever a relação entre dois números inteiros, onde um número é considerado divisível por outro quando a divisão entre eles resulta em um quociente inteiro, sem deixar resto. Esta seção se dedica a apresentar conceitos básicos sobre divisibilidade, úteis para a proposta deste trabalho.

1.2.1 Euclides de Alexandria

Um dos teóricos mais notáveis no desenvolvimento do conceito de divisibilidade é Euclides de Alexandria (cerca 300 a.C.). “Aparentemente, Euclides não criou muitos resultados, mas teve o mérito de estabelecer um padrão de apresentação e rigor na matemática jamais alcançado anteriormente, tido como exemplo a ser seguido (...)” (HEFEZ, 2006, p. 41).

Figura 1.1 – Euclides de Alexandria

Fonte: (E-CáLCULO, -)

Seu trabalho "*Elementos*", trouxe significativas contribuições à geometria e à teoria dos números, incluindo o famoso "Algoritmo de Euclides" para encontrar o maior divisor comum entre dois números inteiros. "Após Euclides, a aritmética estagnou por cerca de 500 anos, ressuscitando com os trabalhos de Diofanto de Alexandria, que viveu por volta de 250 d.C." (HEFEZ, 2006, p. 42).

1.2.2 Definições e propriedades

Reparemos que uma equação do tipo $a \cdot x = b$, com $a, b \in \mathbb{Z}$, dependendo dos valores de a e b, pode ou não possuir soluções inteiras. Quando esta equação possui solução, diz-se então que a é divisível por b e mais precisamente:

Definição 1.21. *Sejam $a, b \in Z$. Dizemos que a divide b se existir $k \in \mathbb{Z}$ tal que $b = a \cdot k$. Se a divide b, diremos também que a é um divisor ou um fator de b ou, ainda que b é um múltiplo de a.*

Usaremos a notação $a \mid b$ para representarmos o caso em que a divide b, do contrário, representamos pela notação $a \nmid b$, o caso de b não ser divisível por a.

Suponhamos que $a \mid b$, (onde $a \neq 0$), e seja $q \in \mathbb{Z}$ de modo que $a \cdot q = b$. Nas condições da Definição 1.21, o inteiro q é único, pois se existisse outro q' de modo que $a \cdot q' = b$, teríamos $a \cdot q = a \cdot q'$ o que resulta em $q = q'$. O inteiro q definido desta forma chama-se de *quociente* de b por a e é indicado por $q = b/a = \frac{b}{a}$. Por outro lado, $0 \mid b$ se, e somente se, $b \neq 0$, neste caso o *quociente* não é único pois $0 \cdot q = 0$, para todo inteiro $q \in \mathbb{Z}$, o quociente $\frac{0}{0}$ é indeterminado. Por isso, vamos descartar o caso em que o divisor é nulo e assumir essa convenção de agora em diante.

Adiante, apresentaremos o conceito de divisibilidade e suas propriedades, visando estabelecer uma base sólida para o entendimento da proposta deste trabalho.

Observação 1.22. *Os divisores de um inteiro qualquer são dois a dois iguais em valor absoluto e de sinais opostos. Dessa forma, se $a \mid b$, então $(-a) \mid b$, pois $b = (-a) \cdot (-q)$, com $(-q) \in \mathbb{Z}$.*

Proposição 1.23. *Quaisquer que sejam os inteiros a, b, c e $d \in \mathbb{Z}$, tem-se:*

1. *$a \mid a$.*
2. *Se $a \mid b$ e se $b \mid c$, então $a \mid c$.*
3. *Se $a \mid b$ e se $c \mid d$, então $a \cdot c \mid b \cdot d$.*
4. *Se $a \mid b$ e se $a \mid c$, então $a \mid (b + c)$.*
5. *Se $a \mid b$ então para $m \in \mathbb{Z}$, tem-se que $a \mid m \cdot b$.*

6. *Se* $a \mid b$ *e* $a \mid c$*, então, para quaisquer* $m, n \in \mathbb{Z}$*, temos* $a \mid (m \cdot b + n \cdot c)$.

Demonstração: 1. Basta observamos que podemos escrever $a \cdot 1 = a$.

2. Por definição, existem inteiros d e d', tais que $a \cdot d = b$ e $b \cdot d' = c$. Substituindo o valor de b dado pela primeira igualdade, temos $c = (a \cdot d) \cdot d' = a \cdot (d \cdot d')$, logo $a \mid c$.

3. Por definição, existem inteiros f e f', tais que $a \cdot f = b$ e $c \cdot f' = d$. Multiplicando ordenadamente ambas as igualdades, temos $a \cdot c \cdot (f \cdot f') = b \cdot d$, donde segue a tese.

4. Existem inteiros d e d', tais que $a \cdot d = b$ e $a \cdot d' = c$. Somando ordenadamente ambas as igualdades, temos $a \cdot (d + d') = b + c$, donde $a \mid b + c$.

5. Se $a \mid b$, existe um inteiro c tal que $a \cdot c = b$. Multiplicando por m, temos $a \cdot (c \cdot m) = b \cdot m$. Portanto $a \mid b \cdot m$.

6. Como $c \mid a$ e $c \mid d$, existem números inteiros e e f tais que $a = c \cdot e$ e $b = c \cdot f$. Logo, $m \cdot a + n \cdot b = m \cdot c \cdot e + n \cdot c \cdot f = c \cdot (m \cdot e + n \cdot f)$. Consequentemente, vemos que $c \mid (m \cdot a + n \cdot b)$.

■

Exemplo 1.24. *Temos os seguintes exemplos:*

1. *Pela Proposição 1.23, temos* $4 \mid 4$, $15 \mid 15$ $10 \mid 10$.

2. *Observe que* $3 \mid 6$, $6 \mid 720$. *Assim, pela Proposição 1.23, temos* $3 \mid 720$.

3. $2 \mid 6$ *e* $5 \mid 15$ *e assim, pela Proposição 1.23,* $10 \mid 90$.

4. *Como* $3 \mid 9$ *e* $3 \mid 27$*, segue da Proposição 1.23 que* $3 \mid (9 + 27)$*, isto é,* $3 \mid 36$.

5. *Uma vez que* $3 \mid 6$*, da Proposição 1.23, segue que* $3 \mid 12 = 6 \cdot 2$, $3 \mid 18 = 6 \cdot 3$, ...

6. *Observe que* $4 \mid 16$ *e* $4 \mid 52$. *Consequentemente, pela Proposição 1.23,* $4 \mid (2 \cdot 16 + 4 \cdot 52) = 240$.

Se os números a e b forem inteiros de modo que b não divida a, é possível então utilizar uma maneira que viabilize efetuar a "divisão" de a por b adquirindo-se um restante, processo este que é finalizado quando obtemos um resto menor que b. Por exemplo, se $a = 752934$ e $b = 7$. Fazemos: $75293 = 10756 \cdot 7 + 1$. Isto pode ser enunciado da seguinte forma: dados dois inteiros a e b, com $b \neq 0$, sempre existem q e r tais que $a = b \cdot q + r$ e $0 \leq r < \mid b \mid$.

Os números q e r são chamados respectivamente de *quociente* e *resto* da divisão de b por a. Notemos que o resto da divisão de b por a é zero se, e somente se $a \mid b$.

Note que b e $r = a - b \cdot q$ possuem $b \cdot q$ como múltiplo e que a condição $0 \leq r < \mid b \mid$ pode ser compreendida, de acordo com LEOPOLD (2015) como a tentativa de encontrarmos um múltiplo de b, menor ou igual a a pois, $a - b \cdot q \geq 0$, de modo que este múltiplo ache-se o mais próximo possível de a. Esta ideia sugere o método de demonstração, no entanto, precisamos inicialmente, estudar um caso particular.

Lema 1.25. *Sejam a e b inteiros tais que $a \geq 0$ e $a > 0$. Então, existem q e r, tais que $a = b \cdot q + r$ e $0 \leq r < b$.*

Demonstração: Consideremos o conjunto $S = \{a - b \cdot x \mid a - b \cdot x \geq 0\}$. Quando $x = 0$, temos que $a - b \cdot x = a \geq 0$ é um elemento mínimo de S, logo $S \neq \emptyset$. Pelo Princípio da Boa Ordem, existe $r = minS$. Como $r \in S$ ele também é da forma $r = a - b \cdot q \geq 0$, para algum $q \in \mathbb{Z}$.

Para mostrar que as condições do enunciado estão verificadas, bastará provar que $r < b$. De fato, se $r \geq b$, teríamos que:

$$a - b \cdot (q + 1) = a - b \cdot q - b = r - b \geq 0,$$

logo, $a - b \cdot (q + 1)$, também pertenceria a S.

Mas $a - b \cdot (q + 1) = r - b < r = min\ S$, uma contradição. ■

Disto segue o resultado a seguir.

Teorema 1.26 (Algoritmo da Divisão)**.** *Se $a, b \in \mathbb{Z}$, com $b \neq 0$, então existem dois únicos q, $r \in \mathbb{Z}$ tais que $a = b \cdot q + r$, com $0 \leq r < \mid b \mid$.*

Demonstração: Inicialmente, mostraremos que podemos determinar q e r quando $b > 0$ e a qualquer. O caso de $a \geq 0$ está dado pelo lema 1.25.

Se $a > 0$, podemos ainda pelo Lema 1.25 determinar q'e r', tais que

$$\mid a \mid = b \cdot q' + r' \ e \ 0 \leq r' < b$$

Se $r' = 0$, temos $- \mid a \mid = a = b \cdot (-q') + 0$, e o par $q = q'$ e $r = 0$ verifica as condições do teorema.

Se $r' > 0$, temos

$$a = - \mid a \mid = b \cdot (-q') - r' = b \cdot (-q') - b + b - r' = b \cdot (-q' - 1) + (b - r')$$

Obviamente, $0 < b - r < b$, logo, os inteiros $q = -q' - 1$ e $r = b - r'$ verificam as condições do enunciado.

Agora provaremos que o resultado também vale quando $b < 0$. Qualquer que seja a, pelo que foi exposto anteriormente, podemos determinar q' e r' tais que

$$a = \mid b \mid \cdot q' + r' \; e \; 0 \leq r' < \mid b \mid$$

Quando $b < 0$, temos que $\mid b \mid = -b$, logo

$$a = \mid b \mid \cdot q' + r' = (-b) \cdot q' + r' = b \cdot (-q') + r',$$

e o inteiros $q = -q'$ e $r = r'$ estão nas condições o enunciado.

Finalmente, provaremos que, se $(q,\ r)$ e $(q',\ r')$ são dois pares de inteiros verificando as condições do enunciado, então $q = q'$ e $r = r'$.

De fato, temos que

$$q \cdot b + r = a = q' \cdot b + r' \tag{1.1}$$

Podemos supor que, por exemplo, que se $r' \geq r$. Da igualdade acima, temos $(q - q') \cdot b = r' - r$. Como $\mid b \mid > r'$, também temos $r' - r < \mid b \mid$. Substituindo, $(q - q') \cdot b < \mid b \mid$ e, tomando módulos,

$$0 \leq \mid q - q' \mid \cdot \mid b \mid < \mid b \mid .$$

Como $\mid b \mid > 0$, podemos cancelar e obtemos $0 \leq \mid q - q' \mid < 1$. Da Proposição 1.19, segue que $\mid q - q' \mid = 0$, isto é, $q = q'$. Da igualdade (1.1), temos que $q \cdot b' + r = q \cdot b + r'$. Cancelando, segue $r = r'$ ■

Exemplo 1.27. *Vamos determinar o quociente e o resto da divisão de 794 por 15. Note que 794 e 15 são números "distantes" e por isso se torna mais difícil encontrar o quociente e o resto da divisãao. Contudo, 79 e 15 são "próximos" e vemos facilmente que* $79 = 15 \cdot 5 + 4$. *Afim de obtermos 794, multiplicamos ambos os lados por 10 e obtemos* $790 = 15 \cdot 50 + 40$. *Somando 4 de ambos os lados temos* $794 = 15 \cdot 50 + 44$. *Como* $44 > 15$, *segue que 44 não é o resto da divisão de 794 por 15. Mas* $44 = 15 \cdot 2 + 14$. *Assim,* $794 = 15 \cdot 50 + 15 \cdot 2 + 14$, *ou seja,* $794 = 15 \cdot 52 + 14$. *Logo, o quociente procurado é 52 e o resto é 14.*

Exemplo 1.28. *Se* $a = 105$ *e* $b = 8$, *então* $q = 13$ *e* $r = 1$, *pois* $105 = 8 \cdot 13 + 1$ *e* $0 \leq 1 < 8$.

A divisibilidade é um pilar da matemática, com aplicações em uma variedade de campos. Sua importância é evidente na teoria dos números, álgebra, criptografia e geometria, contribuindo para a compreensão das propriedades dos números inteiros e impulsionando o progresso matemático ao longo dos séculos.

1.3 Máximo divisor comum

O *máximo divisor comum* é um conceito fundamental na matemática que descreve o maior número inteiro que divide simultaneamente dois ou mais números inteiros. Esta seção explora a definição do *máximo divisor comum*, destaca sua relevância e importância na matemática.

Um inteiro c diz-se um *divisor comum de a e b* se $c \mid a$ e $c \mid b$. O conjunto $D(a,b)$ de todos os divisores comuns de a e b é *limitado superiormente* (pois se $a \neq 0$, para todo elemento $c \in D(a,b)$, temos que $c \leq \mid a \mid$). Consequentemente, $D(a,b)$ tem *máximo*.

Definição 1.29. *Chama-se máximo divisor comum de a e b, o maior de seus divisores comuns, isto é,*

$$mdc(a,b) = max\ D(a,b).$$

O *mdc* de a e b será denotado por $mdc(a,b)$.

Exemplo 1.30. *Os números ± 1, ± 2, ± 4 e ± 8 e ± 16 são os divisores comuns de 16 e 32.*

Teorema 1.31. *Sejam $a, b \in \mathbb{Z}$. Um inteiro positivo d é o máximo divisor comum de a e b se, e somente se verifica*

1. *$d \mid a$ e $d \mid b$.*
2. *Se $d' \mid a$ e $d' \mid b$, então $d' \mid d$.*

Demonstração: Seja $d = mdc(a,b)$. Então, obviamente d verifica a condição (1), então $d \in D(a,b)$. A condição (2) afirma que, se $d' \in D(a,b)$, então $d' \mid d$, logo $d' \leq d$, donde segue que d é o maior dos divisores comuns. Portanto, $d = mdc(a,b)$. ■

Observação 1.32. *É imediato observar que como o máximo divisor comum de a e b não depende da ordem dos termos, temos então $mdc(a,b) = mdc(b,a)$ e em particular $mcd(a,1) = a$.*

Exemplo 1.33. *Os números ± 1, ± 2, ± 4 e ± 8 e ± 16 são os divisores comuns de 16 e 32. Logo, o $mdc(16,32) = 16$.*

Teorema 1.34. *Se $d = mdc(a,b)$, então existem $x_0, y_0 \in \mathbb{Z}$ de maneira que*

$$d = a \cdot x_0 + b \cdot y_0,$$

isto é, o $mdc(a,b) = d$ é uma combinação linear de a e b.

Demonstração: Se $a = b = 0$, então $d = 0$ e qualquer par x_0, y_0 satisfaz $0 = 0 \cdot x_0 = 0 \cdot y_0$.

Se $a \neq 0$ ou $b \neq 0$ (ou ambos), seja:

$$S = \{a \cdot x + b \cdot y \mid x, y \in \mathbb{Z}\}$$

Como $a \cdot a + b \cdot b = a^2 + b^2 \in S$ e $a^2 + b^2 > 0$ (pois $a \neq 0$ ou $b \neq 0$), então em S há elementos estritamente positivos. Se d é o menor desses inteiros, mostraremos que $d = mdc(a, b)$. De fato:

1. Como $d \in S$, então existem $x_0, y_0 \in \mathbb{Z}$, de modo que $d = a \cdot x_0 + b \cdot y_0$. Aplicando o algoritmo da divisão ao elementos a e d,

   $$a = d \cdot q + r \ (0 \leq r < d)$$

   Substituindo d nessa igualdade pelo membro da igualdade anterior:

   $$a = (a \cdot x_0 + b \cdot y_0) \cdot b + r$$

   e então:

   $$r = a \cdot (1 - q \cdot x_0) + b \cdot [q \cdot (-y_0)]$$

   de onde se conclui que $r \in S$. Sendo r positivo e levando em conta que d é o menor dos elementos estritamente positivos de S, então $r = 0$. Donde $a = d \cdot q$ e $d \mid a$. Analogamente, se prova que $d \mid b$.

2. Como $d = a \cdot x_0 + b \cdot y_0$, todo divisor c de a e b é divisor de d.

■

Os elementos de x_0 e y_0 não estão determinados de maneira unívoca. No entanto, quando $a \neq 0$ e $b \neq 0$, o processo das divisões sucessivas permite que encontremos uma solução para tal problema.

Exemplo 1.35. *Seja $a = 15$ e $b = 9$. Como já sabemos:*

$$15 = 9 \cdot 1 + 6$$

$$9 = 6 \cdot 1 + 3$$

$$6 = 3 \cdot 2,$$

onde podemos destacar os principais elementos deste processo. Como $mdc(15, 9) = 3$, tomemos a igualdade onde o resto é igual a 3 e fazemos:

$$3 = 9 - 6 \cdot 1.$$

Como $6 = 15 - 9 \cdot 1$ *(o que obtemos da* 1^a *entre as igualdades anteriores), então:*

$$3 = 9 - (15 - 9 \cdot 1) \cdot 1$$

$$3 = 9 - 15 + 9 \cdot 1$$

$$3 = 15 \cdot (-1) + 9 \cdot 2$$

Isso mostra que $(-1, 2)$ *é solução de* $15 \cdot x + 9 \cdot y = 3$*. Portanto,* $x_0 = -1$ *e* $y_0 = 2$ *são soluções de* $15 \cdot x = 9 \cdot y = 3$*.*

O *máximo divisor comum (mdc)* é um conceito matemático fundamental com ampla relevância em várias áreas, incluindo aritmética, teoria dos números, e criptografia. Autores notáveis, como Euclides, Gauss e Galois, contribuíram para o desenvolvimento e a compreensão dessa área, e o Algoritmo de Euclides permanece como um dos métodos mais poderosos para se calcular o *mdc*. A capacidade de encontrar o maior divisor comum de números inteiros é essencial para resolver problemas matemáticos e explorar a estrutura dos números inteiros.

1.4 Representação dos inteiros

A representação decimal é um método fundamental para expressar números inteiros em base 10, usando um sistema de algarismos que inclui 0 a 9. Esta seção se dedica a explorar o conceito de representação decimal, apresentando alguns conceitos relevantes que contribuem para o desenvolvimento deste trabalho.

O modo convencional de se representar os números inteiros é utilizando o *sistema decimal posicional*, sistema no qual todo número inteiro é representado através de uma sequência formada pelos algarismos 1, 2, 3, 4, 5, 6, 7, 8, 9 e o 0 (que representa ausência de algarismo) e por serem dez algarismos o sistema é denominado por *decimal*, além de *posicional* pelo fato de cada algarismo, possuir além do seu valor, um peso que lhe é atribuído em função da posição que ele ocupa no número, conforme afirma HEFEZ (2006). Esse peso, é sempre uma potência de dez, variando do seguinte modo: o algarismo da extrema direita possui peso 1, o algarismo seguinte (da direita para esquerda) possui peso dois e assim por diante. Por exemplo: o número 19012, em base 10, é a representação de:

$$2 + 1 \cdot 10^1 + 0 \cdot 10^2 + 9 \cdot 10^3 + 1 \cdot 10^4$$

O sistema decimal posicional baseia-se no seguinte resultado.

Teorema 1.36. *Seja* b *um inteiro positivo, com* $b > 1$*. Então todo número inteiro positivo* n *pode ser escrito de forma única da seguinte maneira:*

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b^1 + a_0,$$

onde $a_j \in \mathbb{Z}$*, com* $0 \leq a_j \leq b - 1$ *para todo* $j = 0, 1, 2, \ldots\ k$ *e* $a_k \neq 0$*.*

Demonstração: Obtemos uma expressão do tipo desejado aplicando sucessivamente o algoritmo da divisão, do seguinte modo.

Primeiro dividimos n por b, para obter

$$n = b \cdot q_0 + a_0,\ 0 \leq a_0 \leq b - 1.$$

Dividiremos então q_0 por b para descobrir que

$$q_0 = b \cdot q_1 + a_1,\ 0 \leq a_1 \leq b - 1.$$

Continuamos esse processo para obter

$$q_1 = b \cdot q_2 + a_2,\ 0 \leq a_2 \leq b - 1,$$

$$q_2 = b \cdot q_3 + a_3,\ 0 \leq a_3 \leq b - 1,$$

$$\vdots$$

$$q_{k-2} = b \cdot q_{k-1} + a_{k-1},\ 0 \leq a_{k-1} \leq b - 1,$$

$$q_{k-1} = b \cdot 0 + a_k,\ 0 \leq a_k \leq b - 1.$$

A última etapa do processo ocorre quando um quociente 0 é obtido. Isso é garantido, porque a sequência de quocientes satisfaz

$$n > q_0 > q_1 > q_2 > \ldots > 0,$$

e qualquer sequência decrescente de inteiros não negativos deve eventualmente terminar com um termo igual a 0.

Da primeira equação acima descobriremos que

$$n = b \cdot q_0 + a_0.$$

Em seguida, substituíremos q_0 usando a segunda equação, para obter

$$n = b \cdot (b \cdot q_1 + a_1) + a_0 = b^2 \cdot q_1 + a_1 \cdot b + a_0.$$

Substituindo sucessivamente $q_1,\ q_2,\ \ldots,\ q_{k-1}$, temos

$$n = b^3 \cdot q_2 + a_2 \cdot b^2 + a_1 \cdot b + a_0$$

$$\vdots$$

$$n = b^{k-1} \cdot q_{k-2} + a_{k-2} \cdot b^{k-2} + \ldots + a_1 \cdot b + a_0,$$
$$n = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \ldots + a_1 \cdot b + a_0,$$

onde $0 \leq a_j \leq b-1$, para $j = 0, 1, \ldots, k$ e $a_k \neq 0$, pois $a_k = q \cdot q_{k-1}$ é o último quociente de zero. Consequentemente, encontramos uma expansão do tipo desejado.

Para ver que a expansão é única suponha que tenhamos duas dessas expansões iguais a n, ou seja,

$$n = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \ldots + a_1 \cdot b + a_0$$
$$n = c_k \cdot b^k + c_{k-1} \cdot b^{k-1} + \ldots + c_1 \cdot b + c_0,$$

onde $0 \leq a_k \leq b$ e $0 \leq c_k \leq b$ (e se necessário adicionamos termos iniciais com coeficientes zero para ter o número de termos de acordo).

Subtraindo uma expansão da outra, temos

$$(a_k - c_k) \cdot b^k + (a_{k-1} - c_{k-1}) \cdot b^{k-1} + \ldots + (a_1 - c_1) \cdot b + (a_0 - c_0) = 0.$$

Se as duas expansões forem diferentes, existe um inteiro menor j, $0 \leq j \leq k$, tal que $a_j \neq c_j$. Por isso,

$$b^j \cdot [(a_k - c_k) \cdot b^{k-1} + \ldots + (a_{j+1} + c_{j+1}) \cdot b + (a_j + c_j)] = 0$$

para que

$$(a_k - c_k) \cdot b^{k-j} + \ldots + (a_{j+1} - c_{j+1}) \cdot b + (a_j - c_j) = 0.$$

Resolvendo para $a_j - c_j$, obtemos

$$a_j - c_j = (c_k - a_k \cdot b^{k-j} + \ldots + (c_{j+1} - a_{j+1}) \cdot b$$

$$a_j - c_j = b \cdot [(c_k - a_k) \cdot b^{k-j-1} + \ldots + (c_{j+1} - a_{j+1})]$$

Daí vemos que

$$b \mid (a_j - c_j).$$

Mas como $0 \leq a < b$ e $0 \leq c < b$, sabemos que $-b < a_j - c_j < b$. Consequentemente $b \mid (a_j - c_j)$ que implica que $a_j = c_j$. Isso contradiz o suposto, que as duas expressões são diferentes.

Concluímos que nossa expansão de base b em n é única. ■

A representação dada no Teorema 1.36 é chamada de expansão relativa à base b. Quando $b = 10$, essa expansão é chamada *expansão decimal*, e quando $b = 2$, ela toma o nome de *expansão binária*.

A representação decimal posicional, representa uma prestigiosa limitação de notações, visto que podemos escrever qualquer número inteiro utilizando somente os algarismos

de 0 a 9. Contudo a vantagem mais importante é que tal representação viabiliza que possamos dar regras simples de cálculos aritméticos.

Em teoria, podemos escolher uma base arbitrária e deste modo utilizar o símbolo $(a_m \cdot a_{m-1} \cdot \ldots \cdot a_1 \cdot a_0)_b$ para representar a expressão de a na base b. Geralmente costuma-se omitir mencionar explicitamente quando a base é 10.

Observação 1.37. *No sistema decimal, isto é, b=10, a expressão relativa de um inteiro n é:*

$$n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \ldots + a_1 \cdot 10^1 + a_0$$

$$n = (a_m \cdot a_{m-1} \cdot \ldots \cdot a_1 \cdot a_0)_{10}.$$

De modo que podemos simbolizá-la na forma: $n = 10 \cdot k + a_0,\ com\ k,\ a_0 \in \mathbb{Z}$.

Exemplo 1.38. *Considere n = 918415. Pela Observação 1.37 o número n é escrito da seguinte maneira:*

$$n = 9 \cdot 10^5 + 1 \cdot 10^4 + 8 \cdot 10^3 + 4 \cdot 10^2 + 1 \cdot 10^1 + 5$$
$$n = (9 \cdot 1 \cdot 8 \cdot 4 \cdot 1 \cdot 5)_{10}$$
$$n = 10 \cdot 91841 + 5$$

onde $k = 91841$ *e* $a_0 = 5$

A representação decimal é uma ferramenta fundamental na matemática, essencial para operações aritméticas, notação científica, ciências naturais e ciência da computação. Autores como Al-Khwarizmi, Fibonacci e John Wallis desempenharam papéis significativos na disseminação e desenvolvimento dessa abordagem. A capacidade de expressar números de forma clara e eficaz através da representação decimal é uma conquista matemática que continua a influenciar diversas áreas do conhecimento humano.

1.5 Finalização do capítulo

Ao longo deste capítulo, exploramos diversos aspectos dos números inteiros, desde sua representação decimal até tópicos avançados como o máximo divisor comum. Fica evidente que um sólido conhecimento dos números inteiros é essencial para um entendimento aprofundado da teoria das congruências e suas aplicações.

De fato, como enfatizado por Carl Friedrich Gauss, "Os números governam o universo." A relevância dos números inteiros transcende a matemática pura, permeando

diversas áreas do conhecimento humano. A compreensão do conjunto dos inteiros é fundamental para estabelecer bases sólidas em princípios matemáticos e para explorar aplicações práticas em muitos campos. Como demonstrado ao longo deste capítulo, compreender as propriedades elementares dos números inteiros, como a ordenação, o valor absoluto e o máximo divisor comum, nos será fundamental para desvendar a complexa teoria por trás da determinação de critérios de divisibilidade utilizando congruência. A ordenação e o valor absoluto estabelecem a base para identificar relações de grandeza entre os números e juntamente do conceito de máximo divisor comum, permitem a análise da divisibilidade e a identificação de múltiplos e divisores.

Ao dominar essas propriedades e conceitos, estamos mais aptos a compreender a complexidade da determinação de critérios de divisibilidade por meio da congruência. Juntos, esses conhecimentos nos permitem desvendar padrões numéricos subjacentes, explorar relações entre os números inteiros e compreender a intersecção entre a teoria dos números e a congruência. Isso nos dá as ferramentas necessárias para explorar o mundo das divisibilidades de maneira mais profunda e significativa.

2 Congruências

A congruência é um conceito fundamental na matemática que descreve a relação de equivalência entre números em relação a um módulo específico. Ela permite identificar números que possuem o mesmo "resto" quando divididos pelo mesmo módulo. Essa abordagem é amplamente utilizada em várias áreas da matemática e é fundamental para resolver problemas envolvendo divisibilidade, criptografia, teoria dos números e álgebra.

Neste capítulo apresentaremos essa ferramenta, que fora principiada por Gauss em sua obra *Disquitiones Arithmeticae*, e que é uma das mais importantes na Teoria dos Números. Para tanto, mostraremos a seguir os conceitos relacionados a congruência.

2.1 Carl Friedch Gauss

Johann Friedrih Carl Benz Gauss (1777 − 1855), nasceu em Brunswich, na Alemanha, em 30 de abril de 1777. Estudou na Universidade de Göttingen entre os anos de 1795 à 1798, local onde lecionou matemática e se tornou diretor do Observatório Astronômico daquela instituição, cargos os quais segundo (MEDEIROS, 2015, p. 2) Gauss manteve até o momento de sua morte.

Figura 2.1 – Carl Friedrich Gauss

Fonte: (TARDE,)

As ideias que advieram de Gauss foram, em sua maioria, reunidas em *Disputationes arithmeticae*, onde ele introduz um novo símbolo para referir-se à congruência, enunciando que "se um número m divide a diferença $a - b$ (ou $b - a$) de dois números a e b sem deixar resto, então a e b dizem-se congruentes módulo m" (MEDEIROS, 2015, p. 7) e simbolizou por

$$a \equiv b \ (mod \ m)$$

2.2 Definição e exemplos

Congruência é uma relação entre dois números inteiros, onde estes são considerados congruentes (ou equivalentes) *módulo* m se a diferença entre eles for divisível por m. Formalmente, dados os inteiros a, b e m, dizemos que a *é congruente a* b *módulo* m, representado por $a \equiv b \ (mod\ m)$, se m divide $(a - b)$.

Definição 2.1. *Sejam a, b e $m \in \mathbb{Z}$, tal que $m \neq 0$. Dizemos que a é congruente a b módulo m, se a e b tem o mesmo resto quando divididos por m.*

No caso em que m não divida a-b diremos que a e b são *incongruentes módulo* m e escrevemos $a \not\equiv b \ (mod\ m)$.

Exemplo 2.2. $29 \equiv 15 \ (mod\ 7)$*, pois 29 e 15 tem mesmo resto quando divididos por 7. Em contrapartida,* $29 \not\equiv 6 \ (mod\ 3)$*, pois 29 e 15 não deixam mesmo resto quando divididos por 3.*

Proposição 2.3. *Sejam $a, b \in \mathbb{Z}$, então $a \equiv b \ (mod\ m)$ se, e somente se, $m \mid (a - b)$, ou seja, existe $k \in \mathbb{Z}$, tal que $a = b \cdot k + m$.*

Demonstração: Sejam $a, b \in \mathbb{Z}$. Se $a \equiv b \ (mod\ m)$, então a e b tem mesmo resto quando divididos por m. Assim, existem $q_1,\ q_2,\ r \in \mathbb{Z}$ tais que $a = m \cdot q_1 + r$ e $b = m \cdot q_2 + r$, cm $0 \leq r < \mid m \mid$. Logo, $a - b = m \cdot (q_1 - q_2)$, e portanto, $m \mid (a - b)$.

Reciprocamente, suponhamos que $m \mid (a - b)$. Pelo Teorema 1.26, existem únicos $q_1,\ q_2,\ r_1,\ r_2 \in \mathbb{Z}$ tais que $a = m \cdot q_1 + r_1$ e $b = m \cdot q_2 + r_2$, com $0 \leq r_1,\ r_2 < \mid m \mid$. Assim, $a - b = m \cdot (q_1 - q_2) + (r_1 - r_2)$.

Queremos provar que $r_1 - r_2 = 0$, ou seja, $r_1 = r_2$.

Visto que $m \mid (a - b)$ e $m \mid m \cdot (q_1 - q_2)$, segue da Proposição 1.23 que $m \mid [(a - b) - m \cdot (q_1 - q_2)]$, ou seja, $m \mid (r_1 - r_2)$. Então, claramente, $\mid m \mid \mid (r_1 - r_2)$. Disso e do fato de que $0 \leq \mid r_1 - r_2 \mid < \mid m \mid$, temos $\mid r_1 - r_2 \mid = 0$, ou seja, $r_1 = r_2$, como queríamos demonstrar. ■

Exemplo 2.4. *Temos que* $94 \equiv 24 \ (mod\ 7)$ *e, pela Proposição 2.3, temos* $7 \mid (94 - 24)$*, ou seja,* $94 = 24 + 10 \cdot 7$.

As proposições seguintes decorrem imediatamente da definição de congruência.

2.3 Propriedades

Teorema 2.5. *Seja $\boldsymbol{m}$ um inteiro positivo fixo ($m > 0$) e sejam a, b e c inteiros quaisquer. Temos as seguintes prioridades:*

1. *Reflexiva:* $a \equiv a \ (mod\ m)$
2. *Simétrica Se* $a \equiv b \ (mod\ m)$, *então* $b \equiv a \ (mod\ m)$
3. *Transitiva: Se* $a \equiv b \ (mod\ m)$ *e se* $b \equiv c \ (mod\ m)$, *então* $a \equiv c \ (mod\ m)$

Demonstração: 1. $m \mid 0$ ou $m \mid (a - a) \Rightarrow a \equiv a \ (mod\ m)$

2. Se $a \equiv b \ (mod\ m)$, então $a - b = m \cdot k, \ k \in \mathbb{Z}$. Portanto, $b - a = -(k \cdot m) = (-k) \cdot m \Rightarrow b \equiv a \ (mod\ m)$

3. Se $a \equiv b \ (mod\ m)$ e se $b \equiv c \ (mod\ m)$, então existem inteiros h e k, tais que: $a - b = h \cdot m$ *e* $b - c = k \cdot m$
   Portanto, $a - c = (a + b) + (b - c) = h \cdot m + k \cdot m = (h + k) \cdot m$. E isto significa que $a \equiv c \ (mod\ m)$.

■

2.4 Finalização do capítulo

Um dos teóricos mais importantes no desenvolvimento da teoria da congruência é Carl Friedrich Gauss (1777–1855). Gauss contribuiu significativamente para a compreensão e formalização da congruência e é frequentemente considerado o pioneiro dessa área. Além de Gauss, outros matemáticos como Évariste Galois, Ernst Eduard Kummer e Richard Dedekind também contribuíram para a teoria da congruência e sua aplicação em diversos ramos da matemática.

A congruência é um conceito essencial em várias campos da matemática, sendo fundamental no desenvolvimento de alguns critérios de divisibilidade.

Nesta seção, exploramos conceitos e propriedades fundamentais relacionados às congruências. Introduzimos a noção de congruência, destacando seu símbolo "≡" e abordando suas propriedades essenciais, como reflexividade, simetria e transitividade. Portando essas premissas, preparamo-nos para apresentar a notável realização de Chika Ofili e, subsequemente, detalhar de que maneira os critérios de divisibilidade são estabelecidos por meio da congruência.

3 Divisibilidade por 7: uma descoberta interessante

No ano de 2019, Chika Ofili, um garoto nigeriano com a idade de apenas 12 anos naquela ocasião, morador no Reino Unido e frequentante a Westminster Under School, chamou a atenção das comunidades matemáticas e da mídia em geral. Tudo isso ocorreu devido à notável alegação de que ele havia feito uma descoberta intrigante: um potencial e até então "desconhecido" critério para verificar a divisibilidade por 7, um número inteiro.

Figura 3.1 – Chika Ofili recebendo premiação pela descoberta

Fonte: (SHIMOKAWA, 2020)

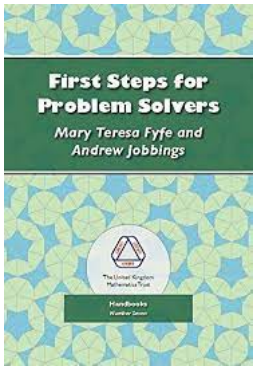
De acordo com a professora de matemática do jovem, Mary Ellis, a descoberta surgiu durante uma tarefa de férias que ela havia proposto a ele. Nessa atividade, ele foi solicitado a explorar os critérios de divisibilidade presentes no livro "First Steps for Problem Solvers", publicado pela United Kingdom Mathematics Trust (UKMT), uma instituição de caridade dedicada a auxiliar a educação matemática de crianças no Reino Unido. Esse livro, conforme descrito por ELLIS (2019), traz métodos ágeis para determinar se um número é divisível de maneira exata por 2, 3, 4, 5, 6, 8 ou 9, antes mesmo de se iniciar o processo de divisão.

No entanto, o ponto intrigante é que esse livro não apresentava nenhum método para verificar a divisibilidade por 7, devido à inexistência de uma abordagem rápida para essa situação específica.

Em um momento de tédio, Chika direcionou sua atenção para a ausência de um método rápido para verificar a divisibilidade por 7 no livro. Nesse contexto, ele teria concebido e proposto seu próprio método, que se baseia na seguinte abordagem:

Se tomarmos o último dígito de qualquer número inteiro, o multiplicarmos por 5 e adicionarmos o número obtido à parte restante do número inicial, obteremos um novo número. Se esse número for divisível por 7, então o número original é divisível por 7.
Vejamos um exemplo para compreender o que de fato Chika Ofili propôs.

Figura 3.2 – First Steps for Problem Solvers - livro que Chika Ofili recebeu de Mary Ellis para leitura durante período de férias



Fonte: (SHIMOKAWA, 2020)

Exemplo 3.1. *Para o número $n = 532$:*
1°) *Passo: Tomemos o número 2, multipliquemos por 5 e adicionemos ao 53, isto é,* $53 + 5 \cdot 2 = 63$.
2°) *Passo: Obtido o número 63, este é divisível por 7, pois* $63 = 7 \cdot q \in \mathbb{Z}$, *sendo* $q = 9$.
Portanto, como 63 é divisível por 7, então 532 é divisível por 7.

Em seguida, "a professora relata que o Chika mostrou seu teste para a turma 8E e nenhum aluno conseguiu encontrar um contra-exemplo" (SHIMOKAWA, 2020, p. 3). No entanto, surgiu a necessidade de fornecer uma demonstração para validar a proposta do jovem. Isso reflete o princípio de que na matemática a verdade é estabelecida através da prova, resultando em uma validação perene, imune a mudanças. Como tal, ainda era necessário fornecer uma prova robusta para a nova abordagem.

Foi então que a professora Ellis decidiu buscar o auxílio de seu irmão, Simon Ellis, também com formação em matemática. Essa colaboração resultou em uma avaliação detalhada da descoberta de Chika. Nesse processo, o método proposto pelo jovem começou a ganhar uma fundamentação algébrica sólida.

3.1 Critérios de divisibilidade por 7

Dados inteiros a e b (com $b \neq 0$), o Algoritmo da Divisão assegura a existência de q e $r \in \mathbb{Z}$, tais que $a = b \cdot q + r$, de maneira simultânea. Entretanto, os critérios de divisibilidade tratam-se de métodos para calcular o resto de uma divisão, sem necessariamente calcular o quociente.

Definição 3.2. *Chama-se critério de divisibilidade todo conjunto de condições que permitem reconhecer se um inteiro dado é divisível por outro.*

O critério mostrado a seguir, "é apresentado num artigo de D. Spence, publicado em 1956, na revista *The Mathematical Gazette*" (TEIXEIRA, 2015). Conforme afirmam DICKSON (1952) e MCDOWELL (2018) *apud* SHIMOKAWA (2020, p. 6) acredita-se que esse método tenha origem em 1861, quando A. Zbikovski publicou um artigo a respeito de testes de divisibilidade no Boletim da Academia de Ciências Físicas de São Petersburgo, onde ele percebeu que um inteiro $\mathbf{N} = a + 10 \cdot k$ é divisível 7 se $k - 2 \cdot a_0$ for divisível por 7.

A proposição apresentada a seguir, tem como base o exposto por AMARAL (2020) e jutamente da análise da Proposição 3.5 serve de base para o desenvolvimento de todo este trabalho.

Proposição 3.3. *O inteiro $n = 10 \cdot k + a_0$, com k, $a_0 \in \mathbb{Z}$, é divisível por 7 se, e somente se, o inteiro $k - 2 \cdot a_0$ é divisível por 7.*

Demonstração: Se $n = 10 \cdot k + a_0$ é divisível por 7, isto é, se $7 \mid 10 \cdot k + a_0$, então, $10 \cdot k + a_0 = 7 \cdot q,\ q \in \mathbb{Z}$.
Daí,
$k - 2 \cdot a_0 = k - 2(7 \cdot q - 10 \cdot k)$
$k - 2 \cdot a_0 = k - 14 \cdot q + 20 \cdot k$
$k - 2 \cdot a_0 = -14 \cdot q + 21 \cdot k$
$k - 2 \cdot a_0 = 7(-2 \cdot q + 3 \cdot k)$
$k - 2 \cdot a_0 = 7 \cdot q_1,\ q_1 = (-2 \cdot q + 3 \cdot k) \in \mathbb{Z}$
E logo, $k - 2 \cdot a_0$ é divisível por 7. Reciprocamente, se $n = k - 2 \cdot a_0$ é divisível por 7, isto é, se $7 \mid k - 2 \cdot a_0$, então $k - 2 \cdot a_0 = 7 \cdot q,\ q \in \mathbb{Z}$.
Daí,
$10 \cdot k + a_0 = 10 \cdot (7 \cdot q + 2 \cdot a_0) + a_0$
$10 \cdot k + a_0 = 70 \cdot q + 20 \cdot a_0 + a_0$
$10 \cdot k + a_0 = 70 \cdot q + 21 \cdot a_0$
$10 \cdot k + a_0 = 7 \cdot (10 \cdot q + 3 \cdot a_0)$
$10 \cdot k + a_0 = 7 \cdot q_2,\ q_2 = (10 \cdot q + 3 \cdot a_0) \in \mathbb{Z}$.
E portanto, $10 \cdot k + a_0$ é divisível por 7. ■

Com base nisto, o seguinte dispositivo prático para testar a divisibilidade de um inteiro por 7, é usual:

Consideremos o **último dígito** de qualquer número inteiro, o **multipliquemos por dois** e **subtraímos o número obtido da parte restante do número inicial**, obtendo um novo número. Se esse número for divisível por 7, então o número original é divisível por 7.

Exemplo 3.4. *Para o número $n = 595$:*
1°) *Passo: Tomemos o número* 5, *multipliquemos por* (-2) *e adicionemos ao* 59, *isto é,*

$53 + (-2) \cdot 5 = 49$
2°) *Passo: Obtido o número 49, este é divisível por 7 pois* $49 = 7 \cdot q \in \mathbb{Z}$, *com* $q = 7$
Portanto, como 49 é divisível por 7, então 595 é divisível por 7.

3.1.1 O método de Chika Ofili: porquê funciona

O método proposto pelo garoto Chika Ofili consiste em tomarmos o **último dígito** de qualquer número inteiro, **o multiplicarmos por 5** e **adicionarmos o número obtido à parte restante do número inicial**, obtendo um novo número. Se esse número for divisível por 7, então o número original é divisível por 7.

Conforme a Observação 1.37, dado um número inteiro n, expresso em base 10, isto é, $n = (a_m \cdot a_{m-1} \cdot \ldots \cdot a_2 \cdot a_1 \cdot a_0)_{10}$ podemos expressá-lo na forma: $n = 10 \cdot k + a_0$. Com isto, podemos propor o seguinte resultado:

Proposição 3.5. *O inteiro* $n = 10 \cdot k + a_0$, *com* $k, a_0 \in \mathbb{Z}$ *é divisível por 7 se, e somente se, o inteiro* $k + 5 \cdot a_0$ *é divisível por 7.*

Demonstração: Se $n = 10 \cdot k + a_0$ é divisível por 7, isto é, $7 \mid 10 \cdot k + a_0$, então, $10 \cdot k + a_0 = 7 \cdot q, \in \mathbb{Z}$.
Daí,
$k + 5 \cdot a_0 = k + 5 \cdot (7 \cdot q - 10 \cdot k)$
$k + 5 \cdot a_0 = k + 35 \cdot q - 50 \cdot k$
$k + 5 \cdot a_0 = 35 \cdot q - 49 \cdot k$
$k + 5 \cdot a_0 = 7 \cdot (5 \cdot q - 7 \cdot k)$
$k + 5 \cdot a_0 = 7 \cdot q_1,\ q_1 = (5 \cdot q - 7 \cdot k) \in \mathbb{Z}$.
E portanto, $k + 5 \cdot a_0$ é divisível por 7.
($\Leftarrow$) Se $n = k + 5 \cdot a_0$ é divisível por 7, isto é, $7 \mid k + 5 \cdot a_0$, então $k + 5 \cdot a_0 = 7 \cdot q,\ q \in \mathbb{Z}$.
Daí,
$10 \cdot k + a_0 = 10 \cdot (7 \cdot q - 5 \cdot a_0) + a_0$
$10 \cdot k + a_0 = 70 \cdot q - 50 \cdot a_0 + a_0$
$10 \cdot k + a_0 = 70 \cdot q - 49 \cdot a_0$
$10 \cdot k + a_0 = 7 \cdot (10 \cdot q - 7 \cdot a_0)$
$10 \cdot k + a_0 = 7 \cdot q_2,\ q_2 = (10 \cdot q - 7 \cdot a_0) \in \mathbb{Z}$.
E portanto, $10 \cdot k + a_0$ é divisível por 7. ■

3.2 O artigo proposto à RPM

AMARAL (2020) propõe, com base em uma análise entre as Proposições (3.3) e (3.5), que observemos alguns fatos:

1. Houve de fato uma descoberta?

2. Temos resultados similares de divisibilidade por 7, na forma $k + x \cdot a_{0,}$ no caso, com $x = (-2)$ e $x = 5$.

3. Em relação ao segundo questionamento, nos proponhamos a pensar se existe $x \in \mathbb{Z}$, com $x \neq (-2)$ e $x \neq 5$, de modo que $7 \mid k + x \cdot a_0$ caso $7 \mid 10 \cdot k + a_0$?

Consideremos que em símbolos, temos:

$$7 \mid 10 \cdot k + a_0 \Leftrightarrow 7 \mid k - 2 \cdot a_0$$
$$7 \mid 10 \cdot k + a_0 \Leftrightarrow 7 \cdot k + 5 \cdot a_0$$

Em relação ao terceiro questionameno, notemos que a diferença entre (-2) e 5 é de 7 unidades. Seguindo esse raciocínio, o próximo inteiro que dista 7 unidades de 5, por exemplo, é o inteiro 12. Dessa forma, seria válido supor que:

$$7 \mid 10 \cdot k + a_0 \Leftrightarrow 7 \mid k + 12 \cdot a_0?$$

Utilizando do método descrito pelos testes rápidos para checar a divisibilidade por 7, apresentados nas Proposições 3.3 e 3.5, temos, por exemplo:

"Considere o **último dígito** de um número inteiro, **multiplique-o por 12**. O resultado **some à parte restante do número inicial**. Se o número obtido for divisível por 7, então o número inicial é divisível por 7".

Exemplo 3.6. *Para o número $n = 595$:*
$1°)$ $5 \cdot 12 = 60$
$2°)$ $59 + 60 = 119$
119 é divisível por 7, portanto, 595 é divisível por 7.

O teste funciona, e a demonstração para isto é análoga àquelas construídas nas Proposição 3.3 e Proposição 3.5.

Desta forma, em relação ao terceiro queestionamento, "o que estamos aqui fazendo é considerar os inteiros congruentes a 5, por exemplo, (o método em questão 'é o de Chika', com o inteiro 5) módulo 7, ou seja, em termos matemáticos, $x \equiv 5 \ (mod\ 7)$" (AMARAL, 2020).

A explicação para esta conjectura se baseia no resultado a seguir, apresentado e demonstrado por AMARAL (2020):

Proposição 3.7. *O inteiro $n = 10 \cdot k + a_0$, com $k,\ a_0 \in \mathbb{Z}$, é divisível por 7 se, e somente se, o inteiro $k + x \cdot a_0$ é divisível por 7, onde $x \equiv 5 \ (mod\ 7)$.*

Demonstração: Temos que
$10 \cdot k + a_0 = 7 \cdot q,\ q \in \mathbb{Z}$ e $7 \mid x - 5$ ou $x = 7 \cdot q_1 + 5.\ q_1 \in \mathbb{Z}$.
Daí,
$k + x \cdot a_0 = k + (7 \cdot q_1 + 5) \cdot (7 \cdot q - 10 \cdot k)$
$k + x \cdot a_0 = k + 49 \cdot q_1 \cdot q - 70 \cdot q_1 \cdot k + 35 \cdot q - 50 \cdot k$
$k + x \cdot a_0 = -49 \cdot k + 49 \cdot q_1 \cdot q - 70 \cdot q_1 \cdot k + 35 \cdot q$
$k + x \cdot a_0 = 7 \cdot (-7 \cdot k + 7 \cdot q_1 \cdot q - 10 \cdot q_1 \cdot k + 5 \cdot q)$
$k + x \cdot a_0 = 7 \cdot q_2,\ q_2 = (-7 \cdot k + 7 \cdot q_1 \cdot q - 10 \cdot q_1 \cdot k + 5 \cdot q) \in \mathbb{Z}$.
E portanto, $k + x \cdot a_0$ é divisível por 7.
Reciprocamente, suponha que $k + x \cdot a_0 = 7 \cdot q_3, q_3 \in \mathbb{Z}$ e $x = 7 \cdot k + 5,\ k \in \mathbb{Z}$.
Então,
$10 \cdot k + a_0 = 10 \cdot (7 \cdot q_3 - x \cdot a_0) + a_0$
$10 \cdot k + a_0 = 70 \cdot q_3 - 10 \cdot (7 \cdot k + 5) \cdot a_0 + a_0$
$10 \cdot k + a_0 = 70 \cdot q_3 - 10 \cdot (7 \cdot k \cdot a_0 + 5 \cdot a_0) + a_0$
$10 \cdot k + a_0 = 70 \cdot q_3 - 70 \cdot k \cdot a_0 - 50 \cdot a_0 + a_0$
$10 \cdot k + a_0 = 70 \cdot q_3 - 70 \cdot k \cdot a_0 - 49 \cdot a_0$
$10 \cdot k + a_0 = 7 \cdot (10 \cdot q_3 - 10 \cdot k \cdot a_0 - 7 \cdot a_0)$
$10 \cdot k + a_0 = 7 \cdot q_4,\ q_4 = (10 \cdot q_3 - 10 \cdot k \cdot a_0 - 7 \cdot a_0) \in \mathbb{Z}$.
E portanto, $10 \cdot k + a_0$ é divisível por 7. ■

Ou seja, dado um inteiro na forma $10 \cdot k + a_0$, este inteiro será divisível por 7 se, e somente se, um inteiro na forma $k + x \cdot a_0$, for divisível por 7, onde há a condição de tomar $x \in \mathbb{Z}$, de maneira que $x \equiv 5\ (mod\ 7)$.

E, temos portanto a seguinte tabela de inteiros que são congruentes a 5 módulo 7.

Tabela 3.1 – Inteiros congruentes a 5 módulo 7

x_n	$x_n - 5$	$7 \mid x_n - 5$	$x_n \equiv 5 (mod\ 7)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
(-9)	$(-9) - 5 = (-14)$	$7 \mid (-14)$	$(-9) \equiv 5\ (mod\ 7)$
(-2)	$(-2) - 5 = (-7)$	$7 \mid (-7)$	$(-2) \equiv 5\ (mod\ 7)$
5	$5 - 5 = 0$	$7 \mid 0$	$5 \equiv 5\ (mod\ 7)$
12	$12 - 5 = 7$	$7 \mid 7$	$12 \equiv 5\ (mod\ 7)$
19	$19 - 5 = 14$	$7 \mid 14$	$19 \equiv 5\ (mod\ 7)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Podemos então indicar um modo de estipular uma infinidade de critérios de divisibilidade pelo inteiro sete, desde que tomemos valores todos mutuamente congruentes a 5 módulo 7 e que por conseguinte satisfazem à condição exposta na Proposição 3.7 Expomos essa determinação na tabela à seguir.

Tabela 3.2 – Critérios de divisibilidade por 7

$\vdots$	$\vdots$
$(-9) \equiv 5\ (mod\ 7)$	$7 \mid 10 \cdot k + a_0 \Leftrightarrow 7 \mid k - 9 \cdot a_0$
$(-2) \equiv 5\ (mod\ 7)$	$7 \mid 10 \cdot k + a_0 \Leftrightarrow 7 \mid k - 2 \cdot a_0$
$5 \equiv 5\ (mod\ 7)$	$7 \mid 10 \cdot k + a_0 \Leftrightarrow 7 \mid k + 5 \cdot a_0$
$12 \equiv 5\ (mod\ 7)$	$7 \mid 10 \cdot k + a_0 \Leftrightarrow 7 \mid k + 12 \cdot a_0$
$19 \equiv 5\ (mod\ 7)$	$7 \mid 10 \cdot k + a_0 \Leftrightarrow 7 \mid k + 19 \cdot a_0$
$\vdots$	$\vdots$

Exemplo 3.8. *Vamos estabelecer alguns critérios de divisibilidade para aferir se $n = 623$ é divisível por 7.*

Tabela 3.3 – Exemplo para $x = -16,\ -9,\ 12,\ e\ 19$.

$x = -16$	$62 - 16 \times 3 = 14$ e $7 \mid 14$
$x = -9$	$62 - 9 \times 3 = 35$ e $7 \mid 35$
$x = 12$	$62 + 12 \times 3 = 98$ e $7 \mid 98$
$x = 19$	$62 + 19 \times 3 = 119$ e $7 \mid 119$

3.3 Finalização do capítulo

Neste capítulo, apresentamos o critério de divisibilidade pelo interio 7 que é comumente exposto na bibliografia matemática, exibimos o critério proposto pelo garoto Chika Ofili bem como sua demonstração e exploramos os critérios de divisibilidade por sete por meio da congruência, comparando o critério convencional com o proposto por Chika Ofili. Ao examinar a relação de congruência existente entre os testes de divisibilidade, destacamos uma correspondência enriquecendo nossa compreensão dos critérios. Essa análise contribui para a teoria dos números, fornecendo uma perspectiva inovadora por meio do que foi proposto por Chika Ofili.

4 Considerações finais

Este trabalho teve como objetivo principal apresentar uma relação de congruência existente na determinação de critérios de divisibilidade pelo inteiro 7, através da análise proposta inicialmente por AMARAL (2020), entre o critério de divisibilidade geralmente exposto na literatura, apresentado por Zbikovski em 1861, e o critério sugerido por Chika Ofili, em 2019.

A investigação da determinação de critérios de divisibilidade pelo inteiro sete através de congruência se configura como uma demonstração matemática de importância significativa. Ao explorar essa linha de pesquisa, estabelece-se uma conexão intrincada entre a teoria dos números e a análise modular, revelando uma profunda compreensão da estrutura numérica subjacente. Através de rigorosos argumentos, a pesquisa estabelece os fundamentos teóricos que desvendam os padrões de divisibilidade associados ao número sete.

Por meio da aplicação de técnicas de congruência, é possível traçar relações sistemáticas entre os números inteiros e suas representações modulares. Essa abordagem revela propriedades distintas que não apenas enriquecem a teoria dos números, mas também têm potencial aplicação em campos práticos.

Portanto, a pesquisa sobre a determinação de critérios de divisibilidade pelo inteiro sete por meio de congruência transcende o mero exercício teórico, configurando-se como uma demonstração eloquente inter-relação entre matemática pura e aplicações concretas, contribuindo assim para o avanço do conhecimento matemático e suas implicações práticas.

No que concerne à empregabilidade da congruência na definição de critérios de divisibilidade, observa-se uma ampla abordagem no panorama acadêmico. Entretanto, é imperativo destacar que o material consultado revelou-se, em sua maioria, de complexidade elevada, dificultando a compreensão substancial do tema em ques

Contudo, são inúmeras as aplicações de divisibilidade e congruência, as quais seria inviável apresentar em um trabalho deste gênero, contudo, quanto ao estudo de divisibilidade pelo inteiro 7, propomos como uma possível continuação deste trabalho, a determinação de critérios de divisibilidade por 7 através de uma análise de $\mathbb{Z}_7$.

Referências

AMARAL, L. F. C. Divisibilidade por 7: um novo método? *Revista do Professor de Matemática*, n. 101, 2020. Citado 4 vezes nas páginas 33, 34, 35 e 38.

DICKSON, L. E. *History of the theory of numbers. Vol. 1, Divisibility and primality.* [S.l.]: Chelsea Publishing Company, 1952. Citado na página 33.

E-CáLCULO. Título: " euclides de alexandria (por volta de 325 a.c. - 265 a.c.)". disponível em: http://ecalculo.if.usp.br/historia/euclides.htm acesso em: 15/02/2023. –. Citado na página 16.

ELLIS, M. E. Título: "chika's test". disponível em: https://www.westminsterunder.org.uk/news/chikas-test/. acesso em: 07/09/2022. 2019. Citado na página 31.

HEFEZ, A. *Elementos de aritmética*. [S.l.]: Sociedade Brasileira de Matemática, 2006. Citado 3 vezes nas páginas 16, 17 e 23.

LEOPOLD, G. L. *Congruência e aplicações*. Dissertação (Mestrado) — Brasil, 2015. Citado na página 19.

MCDOWELL, E. Divisibility tests: A history and user's guide. *Convergence (May 2018)[online]. Dostupné z https://www. maa. org/press/periodicals/convergence/divisibility-tests-a-history-and-users-guide*, 2018. Citado na página 33.

MEDEIROS, J. M. G. d. Congruência e aplicações. 2015. Citado na página 28.

MILIES, F. C. P.; COELHO, S. P. Números: Uma introdução à matemática. 1998. Citado 2 vezes nas páginas 13 e 14.

SHIMOKAWA, E. Y. Teste de chika: Um critério geeal de divisibilidade. 2020. Citado 3 vezes nas páginas 31, 32 e 33.

TARDE, P. A. Título: "príncipe da matemática deixou grande legado para a humanidade". disponível em: https://atarde.com.br/opiniao/principe-da-matematica-deixou-grande-legado-para-a-humanidade-948641 acesso em: 29/04/2023. Citado na página 28.

TEIXEIRA, R. E. C. Critérios de divisibilidade por 7 e por 11. *Tribuna das Ilhas*, IAIC-Informação, Animação e Intercâmbio Cultural, p. 9–9, 2015. Citado na página 33.