UNIVERSIDADE ESTADUAL DO PIAUÍ – UESPI
CENTRO DE CIÊNCIAS DA NATUREZA – CCN
LICENCIATURA PLENA EM MATEMÁTICA

Thiago Brito Lustosa

MÚLTIPLOS E DIVISORES: UMA APLICAÇÃO NA CRIPTOGRAFIA

TERESINA
2023

Thiago Brito Lustosa

MÚLTIPLOS E DIVISORES: UMA APLICAÇÃO NA CRIPTOGRAFIA

Trabalho de Conclusão de Curso apresentado ao Curso Superior de Licenciatura em Matemática da Universidade Estadual do Piauí, em cumprimento às exigências legais como requisito parcial à obtenção do título de Licenciado em Matemática.

Orientador: Prof.º Dr. Afonso Norberto da Silva.

Teresina
2023

L968m Lustosa, Thiago Brito.
Múltiplos e divisores: uma aplicação na criptografia / Thiago Brito Lustosa. – 2023.
37 f. : il.

Monografia (graduação) – Universidade Estadual do Piauí – UESPI, Licenciatura em Matemática, *Campus* Poeta Torquato Neto, Teresina-PI, 2023.
"Orientador Prof. Dr. Afonso Norberto da Silva."

1. Múltiplos. 2. Divisores. 3. Criptografia RSA. 4. Divisibilidade. I. Título.

CDD: 510.07

Ficha elaborada pelo Serviço de Catalogação da Biblioteca Central da UESPI
Nayla Kedma de Carvalho Santos (Bibliotecária) CRB-3ª/1188

AGRADECIMENTOS

Agradeço, primeiramente, a Deus pela oportunidade de realização de mais um sonho. Sem Ele nada seria possível.

A meus pais, José Lustosa e Maria dos Milagres, pelos valores consolidados em minha formação.

A minha esposa Moara Regina por acreditar e me incentivar nos momentos difíceis.

A meus filhos, Ana Beatriz e Guilherme, pela paciência e o respeito pela minha ausência em alguns momentos dessa jornada.

A meu Tio Chico Lustosa que com certeza foi instrumento de Deus me dando um suporte necessário pra realização desse sonho.

Ao Professor Afonso pela sua orientação e comprometimento.

A meus amigos de turma, em especial Mylla e Osmarina, que participaram de tantos momentos importantes.

Aos professores, Raimundo e Alessando, membros da banca, que muito contribuíram na conclusão deste trabalho.

"*Aquele que vive a coerência, a Palavra de Deus tem eficácia na sua vida e não gera morte, mas sim vida.*"

Padre Bruno Antônio

RESUMO

Neste trabalho, apresentamos a aplicabilidade dos múltiplos e divisores. Exploramos as diferentes ideias inerentes a multiplicação e divisão. Assim como a relação dessas operações no Algoritmo da Divisão. Abordamos a utilização da Criptografia RSA como um exemplo prático no uso dos múltiplos e divisores. Realizamos uma breve fundamentação teórica e a aplicação dos mesmos para exemplificar a relevância de tais conceitos.

Palavras-chave: Múltiplos; divisores; divisibilidade; Criptografia RSA.

ABSTRACT

In this work, we present the applicability of multiple and dividers. We explore the different ideas intrinsic to multiplication and Division. As well as the relationship of these operations in the Division Algorithm. We address the use of RSA Cryptography as a practical example in the use of multiplex and divisors. We provide a brief theoretical foundation and their application to exemplify the relevance of such concepts.

Keywords: multiple; dividers; divisibility; RSA encryption.

Sumário

1 INTRODUÇÃO

As necessidades práticas estimulam o desenvolvimento das ciências, foi assim no passado e persiste nos dias atuais. Assim, podemos definir a matemática como uma ciência dinâmica, num processo de construção diário. Diante disso uma estreita relação foi sendo desenvolvida entre a Teoria dos Números e o conceito de divisibilidade.

> A Matemática, sob as formas da Aritmética e da Geometria rudimentares, nasceu para suprir as necessidades de contagens, facilitar as transações comerciais e guiar os construtores de edificações, monumentos, canais de irrigação e outras obras das primeiras civilizações. Isso ocorreu em meados do quarto milênio a.C., na Mesopotâmia e no Egito, e, alguns séculos depois, na Índia e na China. Ela era, então, puramente indutiva, fruto do raciocínio que o homem aplicava sobre aquilo que observava ou carecia. ([1], p. 28)

De fato, um dos maiores desafios enquanto professor de matemática é despertar no aluno o seu interesse pela disciplina. Em alguns conteúdos a forma abstrata apresentada e sem o uso prático dificulta aproximar os alunos desses conceitos matemáticos.

Durante muito tempo a Teoria dos Números – um ramo da matemática com foco nas propriedades dos números em geral, e em particular dos números inteiros – foi vista como uma parte da matemática sem aplicações práticas, mas com o advento da internet e a necessidade de proteger as informações, ela se mostrou uma solução pra viabilizar a proteção da troca de mensagens entre usuários de aplicativos e transações financeiras seguras. Por exemplo, a Criptografia RSA que utiliza uma ideia simples: dados dois números primos p e q, o seu produto é um número n. Esse número é a chave pública, enquanto p e q são as chaves privadas. Conhecidos p e q, é relativamente fácil achar n, pois basta multiplicar p por q, mas é difícil achar p e q a partir de n, pois este precisará ser fatorado e isso pode levar muito tempo.

Com o objetivo de ampliar a compreensão dos alunos do Ensino Médio em relação ao Algoritmo da Divisão, o desenvolvimento deste trabalho iniciou com intuito de compreender as situações-problema em que os conceitos de múltiplos e divisores permitem resolver, bem como sua aplicação representou uma parcela significativa no desenvolvimento da Teoria dos Números.

O trabalho é organizado como segue: no segundo capítulo mostraremos as ideias utilizadas na multiplicação e divisão e alguns problemas para exemplificar. Bem como, as ideias que diferenciam o MMC do MDC com seus respectivos exemplos.

No terceiro capítulo, veremos a definição de divisibilidade e o teorema do Algoritmo da Divisão, definição de múltiplos e divisores comuns, com exemplos e ainda alguns corolários.

No último capítulo, iremos mostrar algumas aplicações dos múltiplos, divisores e uma aplicação prática do Algoritmo da Divisão que visa contextualizar o conteúdo no Ensino Médio e despertar o interesse do aluno pela disciplina, colocando a matemática como uma das ciências responsável pelo desenvolvimento da sociedade.

2 USO DA MULTIPLICAÇÃO E DIVISÃO

A definição de divisibilidade é fundamental na matemática e está intrinsecamente ligada a relação entre múltiplos e divisores de um número. Antes de abordar os conceitos de múltiplos e divisores, iremos compreender os significados da multiplicação e divisão no contexto cotidiano para só então abordamos esses conceitos.

"Em relação aos números, os estudantes do Ensino Fundamental têm a oportunidade de desenvolver habilidades referentes ao pensamento numérico, ampliando a compreensão a respeito dos diferentes campos e significados das operações." ([2], p. 529)

De fato, é importante para o aluno compreender os significados das operações e como elas se relacionam, pois isso irá ampliar e consolidar o uso em diferentes contextos sociais e matemáticos. Essa relação será percebida ao apresentarmos a definição de divisibilidade.

Segundo [3] a multiplicação está relacionada a ideia de adição de parcelas iguais, formação retangular e proporção, enquanto as ideias de distribuição equitativa (repartição em partes iguais) ou de medida (quantas vezes uma quantidade cabe em outra) estão relacionadas à divisão. Para melhor exemplificar a identificação das ideias de multiplicação e divisão, citaremos dois problemas.

Problema 1. Numa competição de kart, Marcus Avião dá uma volta completa na pista oval em 28 segundos, enquanto José Lindinho leva 32 segundos para completar uma volta. Quando Marcus Avião completar a volta número 40, José Lindinho estará completando qual volta?[1]

Para chegarmos à solução desse problema devemos saber quanto tempo Marcus Avião gastou até o término da volta 40, ou seja, a ideia de adição de parcelas iguais:

$$\underbrace{28 + 28 + \cdots + 28}_{40\ vezes} = 40 \text{ x } 28 = 1.120 \text{ segundos}$$

Sabendo o resultado do produto e sabendo que José Lindinho completa uma volta em 32 segundos, veremos quantas vezes 32 segundos cabe em 1.120 segundos, ou seja:

$$1.120 \div 32 = 35$$

Logo, quando Marcus Avião estiver completando a volta 40, José Lindinho completará a volta 35.

Problema 2. Um paciente necessita de reidratação endovenosa feita por meio de cinco frascos de soro durante 24h. Cada frasco tem um volume de 800ml de soro. Nas primeiras quatro horas, deverá receber 40% do total a ser aplicado. Cada mililitro de soro corresponde a 12 gotas. Qual

[1] VUNESP-2002

o número de gotas por minuto que o paciente deverá receber após as quatro primeiras horas será?[2]

Como são 5 frascos de 800ml, temos um total de 5 x 800 = 4.000ml.

Sabemos que 1ml correspondem a 12 gostas. Logo, 4.000ml correspondem a 4.000 x 12 = 48.000 gotas.

Nas primeiras 4 horas o paciente deverá receber 40% do total, ou seja, 40% x 48.000 = 19.200 gotas.

Do total sobram 48.000 – 19.200 = 28.800 gotas a serem aplicadas durante as 20 horas restantes do dia. Cada hora tem 60 minutos. 20 horas, portanto, correspondem a 20 x 60 = 1.200 minutos.

Ou seja, restam 28.800 gotas para serem aplicadas ao longo de 1.200 minutos. Isso dá um total de 28.800 ÷ 1.200 = 24 gotas por minuto.

Esses tipos de problemas exemplificam a necessidade de privilegiar atividades que possibilitem ao aluno ampliar a compreensão do significado das operações, ou seja, atividades que permitam reconhecer relações entre os significados e as diferentes operações.

3 CIRCUNSTÂNCIAS DO MMC E MDC

No Ensino Fundamental é objetivo do professor conduzir o aluno a reconhecer e distinguir números primos de números compostos e escrever números compostos como decomposição de fatores primos, pois a decomposição será muito útil na obtenção do Mínimo Múltiplo Comum e Máximo Divisor Comum entre dois números. Mais do que calcular o MMC e o MDC é necessário ao aluno reconhecer nas situações-problema qual o método ele irá utilizar para solucionar o problema. Assim, utilizaremos três problemas para exemplificar quais ideias devem ser compreendidas para o uso do MMC ou do MDC nas resoluções.

Problema 3. Rui e Roberto fazem a segurança noturna de uma empresa e devem acionar o relógio de controle ao final de cada ronda, que tem percursos diferentes para cada um. A ronda de Rui dura 30 minutos e a de Roberto, 40 minutos. Se eles acionarem simultaneamente o relógio de controle às 23h45min, então um novo acionamento simultâneo só deverá se repetir que horas?[3]

[2] ENEM-2016
[3] VUNESP-2005

Para [3] um número natural será múltiplo de outro se for o resultado da multiplicação desse número por algum número natural. Quando temos 2 números x e y, e listamos os múltiplos de cada um deles que são infinitos, podemos ter múltiplos em comum entre os dois. Justamente essa ideia de "encontro" ou "próximo encontro" será utilizada para solucionar os problemas 3 e 4.

Iniciamos indicando o conjunto dos múltiplos de 30 e 40:

m(30) = {0, 30, 60, 90, 120, 150, 180, 210, 240, ...}

m(40) = {0, 40, 80, 120, 160, 200, 240, 280, 320, ...}

Assim, visualizamos que o menor múltiplo de 30 minutos e 40 minutos é igual a 120 minutos que é igual a 2 horas. Como Rui e Roberto acionaram os relógios às 23h45min, então o próximo acionamento será: 23h45min + 2h = 1h45min.

Problema 4. Sob a orientação de um mestre de obras, João e Pedro trabalharam na reforma de um edifício. João efetuou reparos na parte hidráulica nos andares 1, 3, 5, 7, e assim sucessivamente, de dois em dois andares. Pedro trabalhou na parte elétrica nos andares 1, 4, 7, 10, e assim sucessivamente, de três em três andares. Coincidentemente, terminaram seus trabalhos no último andar. Na conclusão da reforma, o mestre de obras informou, em seu relatório, o número de andares do edifício. Sabe-se que, ao longo da execução da obra, em exatamente 20 andares, foram realizados reparos nas partes hidráulicas e elétricas por João e Pedro. Qual é o número de andares desse edifício?[4]

Notamos que João avança de dois em dois andares. Já Pedro avança de três em três andares. Ao encontrarmos o MMC (2,3) = 6, concluímos que a cada 6 andares eles se encontram. A primeira vez que eles se encontram é no primeiro andar. Depois disso, eles ainda vão se encontrar 19 vezes até o vigésimo encontro. Portanto, serão necessários 1 + 19 x 6 = 1 + 114 = 115 andares para possibilitar os 20 encontros. Logo, o número de andares desse edifício é 115. Assim, podemos perceber mais uma vez a ideia de "encontro" remeter ao Mínimo Múltiplo Comum como princípio pra solução da questão.

Problema 5. O gerente de um cinema fornece anualmente ingressos gratuitos para escolas. Este ano serão distribuídos 400 ingressos para uma sessão vespertina e 320 ingressos para uma sessão noturna de um mesmo filme. Várias escolas podem ser escolhidas para receberem ingressos. Há alguns critérios para a distribuição dos ingressos:

1) cada escola deverá receber ingressos para uma única sessão;
2) todas as escolas contempladas deverão receber o mesmo número de ingressos;

[4] ENEM-2016

3) não haverá sobra de ingressos (ou seja, todos os ingressos serão distribuídos).

Qual o número mínimo de escolas que podem ser escolhidas para obter ingressos, segundo os critérios estabelecidos?[5]

Num problema cujo conteúdo é o MDC, é importante evidenciar aos alunos o surgimento de alguns critérios exigidos. A princípio, fala-se de uma "uniformidade" (no texto isto surge quando se diz que são os mesmos números de ingressos para as escolas contempladas) e sempre há uma ideia de "divisão exata", ou seja, todos os ingressos serão distribuídos. Para sabermos o número mínimo de escolas, precisamos saber a quantidade máxima de ingressos que cada escola poderá receber, ou seja, usaremos o maior divisor comum dos ingressos.

Iniciamos indicando o conjunto dos divisores de 320 e 400:

D (320) = {1, 2, 4, 5, 8, 10, 16, 20, 32, 40, 64, 80, 160, 320}

D (400) = {1, 2, 4, 5, 8, 10, 16, 20, 25, 40, 50, 80, 100, 200, 400}

Note que os números 1, 2, 4, 5, 8, 10, 16, 20, 40 e 80 são divisores de 320 e 400, ou seja, eles são divisores comuns. Como precisamos saber a quantidade máxima de ingressos, ou seja, o máximo divisor comum de 320 e 400 que é 80. Logo, 80 é número máximo que cada escola deverá receber.

Para sabermos o número mínimo de escolas, precisamos efetuar a divisão do número de ingressos de cada sessão pelo número máximo de ingressos que cada escola deve receber, ou seja, 400 ÷ 80 = 5 e 320 ÷ 80 = 4. Logo, o número mínimo de escolas que podem ser escolhidas será 5 + 4 = 9 escolas.

Mais uma vez verificamos a necessidade de privilegiar atividades que possibilitem ao aluno ampliar a compreensão dos significados, ou seja, atividades que permitam reconhecer relações entre as ideias dos textos e as diferentes estratégias de soluções.

[5] ENEM-2015

4 DIVISIBILIDADE

A Teoria dos Números é a área da matemática responsável por estudar as propriedades dos números inteiros, assim como suas implicações. Muitas proposições e teoremas fundamentais precisam das propriedades de divisibilidade para poderem ser demonstrados.

Utilizaremos, usualmente, $\mathbb{N}$ e $\mathbb{Z}$ para representar respectivamente os conjuntos dos números naturais e inteiros.

Notação:

1. Denotamos por $\mathbb{Z}^* = \{z \in \mathbb{Z}, z \neq 0\}$, que denominamos como conjunto dos números inteiros não nulos.
2. Denotamos por $\mathbb{Z}_+ = \{z \in \mathbb{Z}, z \geq 0\}$, que denominamos como conjunto dos números inteiros não negativos.
3. Denotamos por $\mathbb{Z}_- = \{z \in \mathbb{Z}, z \leq 0\}$, que denominamos como conjunto dos números inteiros não positivos.

Definição 1: Dados os números inteiros a e b definimos a operação multiplicação como

1. se $a, b \in \mathbb{Z}_+$ é uma multiplicação de números tal que $a \cdot b = \underbrace{a + a + \cdots + a}_{b\ parcelas}$.
2. se $a \in \mathbb{Z}_-$ e $b \in \mathbb{Z}_+$ definimos $a \cdot b = \underbrace{a + a + \cdots + a}_{b\ parcelas}$.
3. se $a \in \mathbb{Z}_-$ e $b \in \mathbb{Z}_-$ definimos $a \cdot b = (-a) \cdot (-b)$.

Definição 2: Sejam a e b dois inteiros, com $a \neq 0$. Diz-se que a divide b se, e somente se, existe um inteiro q tal que $b = a \cdot q$

Ainda podemos dizer:

- ✓ a é um divisor ou fator de b
- ✓ b é um múltiplo de a
- ✓ b é divisível por a

Observe que a notação a|b não representa nenhuma operação em $\mathbb{Z}$, nem representa uma fração. Trata-se de uma sentença que diz ser verdade que existe um número q inteiro tal que $b = a \cdot q$.

A negação dessa sentença é representada por $a \nmid b$, leem-se (a não divide b), significando que não existe nenhum número inteiro q tal que $b = a \cdot q$.

Proposição 1: Se $a|b$, então $-a|b$.

Demonstração:

Pela definição (2),

Se $a|b$, existe $c \in \mathbb{Z}$ tal que $b = a \cdot c$. Como $a \cdot c = (-a) \cdot (-c)$. Temos $b = (-a) \cdot (-c)$. Logo, $-a|b$.

Exemplo 1:

2|10, pois 10 = 2·5

–3|18, pois 18 = (–3)·(–6)

7|–14, pois –14 = 7·(–2)

3∤10, pois ∄ q ∈ ℤ ; 10 = 3·q

Teorema 1: Quaisquer que sejam os inteiros a, b e c, tem-se:

1) a|0 com a ≠ 0, 1|a e a|a com a ≠ 0

2) Se a|1, então a = ±1

3) Se a|b e se c|d, então ac|bd

4) Se a|b e se b|c, então a|c

5) Se a|b e se b|a, então a = ±b

6) Se a|b, com b ≠ 0, então | a | ≤ | b |

7) Se a|b e se a|c, então a|(bx ± cy), ∀ x, y ∈ ℤ

Os teoremas 1, 5, 6 e 7 têm suas demonstrações conforme [4].

Demonstração:

1) Pela definição (2):

a. Se $a|0$, existe $q_1 \in \mathbb{Z}$ tal que $0 = a \cdot q_1$, dai $q_1 = 0$, ou seja, $0 = a \cdot 0$;

b. Se $1|a$, existe $q_2 \in \mathbb{Z}$ tal que $a = 1 \cdot q_2$, dai $q_2 = a$, ou seja, $a = 1 \cdot a$;

c. Se $a|a$, existe $q_3 \in \mathbb{Z}$ tal que $a = a \cdot q_3$, dai $q_3 = 1$, ou seja, $a = a \cdot 1$.

2) Se $a|1$, então existe um $q \in \mathbb{Z}$ tal que $1 = a \cdot$ q implicando nas seguintes possibilidades:

$a = 1$ e $q = 1$ ou $a = -1$ e $q = -1$. Logo $a = \pm 1$.

3) Se $a|b$ e se $c|d$, então pela definição de divisibilidade existem os inteiros q_1 e q_2 tais que:

$$b = a \cdot q_1, \text{ com } q_1 \in \mathbb{Z}. \qquad (1)$$

$$d = c \cdot q_2, \text{ com } q_2 \in \mathbb{Z}. \qquad (2)$$

Multiplicando membro a membro (1) e (2), tem-se

$$bd = (a \cdot c)(q_1 \cdot q_2) \Longrightarrow ac|bd.$$

4) Se $a|b$ e se $b|c$, então pela definição de divisibilidade existem os inteiros q_1 e q_2 tais que:

$$b = a \cdot q_1, \text{ com } q_1 \in \mathbb{Z}. \quad (3)$$

$$c = b \cdot q_2, \text{ com } q_2 \in \mathbb{Z}. \quad (4)$$

Multiplicando membro a membro (3) e (4), tem-se

$$bc = (a \cdot b)(q_1 \cdot q_2) \Longrightarrow c|a(q_1 \cdot q_2)$$
$$\Longrightarrow a|c.$$

5) Se $a|b$ e se $b|a$, então pela definição de divisibilidade existem os inteiros q_1 e q_2 tais que:

$$b = a \cdot q_1, \text{ com } q_1 \in \mathbb{Z}. \quad (5)$$
$$a = b \cdot q_2, \text{ com } q_2 \in \mathbb{Z}. \quad (6)$$

Substituindo (5) em (6),

$$a = a(q_1 \cdot q_2) \Longrightarrow q_1 \cdot q_2 = 1 \Longrightarrow q_1|1.$$

Pelo item 2 do Teorema 1 implica que $q_1 = \pm 1$. Logo, $a = \pm b$.

6) Se $a|b$ com $b \neq 0$, então por definição existe $q \in \mathbb{Z}$ tal que $b = a \cdot q$, aplicando o módulo em ambos os membros e utilizando as propriedades básicas de módulo, temos que:

$$|b| = |a \cdot q| = |a| \cdot |q| \quad (7)$$

Com $a \neq 0$, por definição e por hipótese temos que $b \neq 0$. Como $q \neq 0$, então $1 \leq |\,q\,|$, daí multiplicando por $|a|$, tem-se

$$|a| \leq |q| \cdot |a|. \qquad (8)$$

Logo de (7) e (8) obtemos que:

$$|a| \leq |b|.$$

7) Se $a|b$ e se $a|c$, então pela definição de divisibilidade existem os inteiros q_1 e q_2 tais que:

$$b = a \cdot q_1, \text{ com } q_1 \in \mathbb{Z}. \qquad (9)$$

$$c = a \cdot q_2, \text{ com } q_2 \in \mathbb{Z}. \qquad (10)$$

Portanto, quaisquer que sejam os inteiros x e y, multiplicando (9) por x e (10) por y e subtraindo membro a membro, obtemos:

$$bx - cy = aq_1x - aq_2y = a(q_1x - q_2y)$$

então $a|(bx - cy)$, para todo x e y inteiros. A adição é feita de forma análoga. Portanto, $a|(bx \pm cy)$. C.Q.D.

Faremos a verificação que a relação de divisibilidade em $\mathbb{Z}$ não é uma relação de equivalência. Apesar da divisibilidade em $\mathbb{Z}$ ser reflexiva e transitiva respectivamente pelos itens (1.c) e (4), ela não é simétrica.

Definição 3: Uma relação binária *R* num conjunto A é qualquer subconjunto do produto cartesiano A×A.

Notação: Se *R* é uma relação binária em A e se $(a, b) \in R$, escrevemos aRb, isto é,

$$(a, b) \in R \Leftrightarrow aRb.$$

Definição 4: Uma relação *R* em A diz-se relação de equivalência se possuir as seguintes propriedades:

1. *reflexiva*: aRa, para todo $a \in$ A;

2. *simétrica*: se $a, b \in$ A e aRb, então bRa;
3. *transitiva*: para $a, b, c \in$ A, se aRb e bRc, então aRc.

Vamos mostrar em seguida que a divisibilidade em $\mathbb{Z}$ não é uma relação de equivalência. De fato:

1. Vale a reflexiva: para todo $a \in \mathbb{Z}$, $a = ac$ com $c = 1 \in \mathbb{Z}$, portanto aRa.
2. Não vale a simétrica: Se $a, b \in \mathbb{Z}$ e $a|b$, temos que, $b = a \cdot c_1$, com $c_1 \in \mathbb{Z}$. Se b dividisse a, teríamos $a = b \cdot c_2$, com $c_2 \in \mathbb{Z}$ e assim $a = a \cdot c_1 \cdot c_2 \Rightarrow a = a \cdot c \Rightarrow c = c_1 \cdot c_2 = 1$, o que significa que $c_1 = c_2 = 1$ ou $c_1 = c_2 = -1$. Assim, podemos concluir que só vale a simétrica quando $a = b$ ou $a = -b$. Portanto, não vale a simétrica para quaisquer $a, b \in \mathbb{Z}$ onde $a|b$.
3. Vale a transitiva: Se $a, b, d \in \mathbb{Z}$, $a|b$ e $b|d$, temos que $b = a \cdot c_1$ e $d = b \cdot c_2$, com $c_1, c_2 \in \mathbb{Z}$. Logo, $d = a \cdot c_1 \cdot c_2 \Rightarrow d = a \cdot c$, com $c_1 c_2 = c \in \mathbb{Z}$. Portanto, $a|d$.

Exemplo 2: 2|10 e 10∤2, aqui verificamos um contraexemplo da simétrica na relação de divisibilidade em $\mathbb{Z}$.

2|10, pois 10 = 2·5, mas 10∤2 pois ∄ q ∈ $\mathbb{Z}$; 2 = 10 · q.

Além do teorema anterior, iremos apresentar outros dois teoremas que se utilizam dos mesmos artifícios para suas demonstrações e são bastante utilizados em resoluções de questões.

Teorema 2: Sejam a, b e c inteiros. Se $a|b$, então $a|bc$.

Prova: Se $a|b$, então por definição existe o inteiro q tal que:

$$b = a \cdot q \qquad (11)$$

com $q \in \mathbb{Z}$.

Multiplicando c em ambos os membros de (1), teremos:

$$bc = a(cq).$$

Fazendo $cq = q_1$, temos que $bc = a \cdot q_1$. Portanto, $a|bc$.

Teorema 3: Sejam a, b e c inteiros. Se $a|b$ e se $a|c$, então $a^2|bc$.

Prova: Se $a|b$ e se $a|c$, então por definição existem os inteiros q_1 e q_2 tais que:

$$b = a \cdot q_1 \text{ e } c = a \cdot q_2 \qquad (12)$$

com q_1 e $q_2 \in \mathbb{Z}$.

Multiplicando membro a membro (2), teremos:

$$bc = aa(q_1q_2).$$

Portanto, $bc = a^2 \cdot (q_1q_2)$. Logo, $a^2|bc$.

5 CONJUNTO DOS DIVISORES DE UM INTEIRO

O conjunto de todos os divisores de um inteiro qualquer a indica-se por D(a), ou seja:

$$D(a) = \{x \in \mathbb{Z}^* ; x|a\}$$

onde $\mathbb{Z}^*$ denota o conjunto dos inteiros não nulos ($\neq 0$).

Exemplo 2:

$D(0) = \{x \in \mathbb{Z}^* ; x|0\} = \mathbb{Z}^*$

$D(3) = \{x \in \mathbb{Z}^* ; x|3\} = \{\pm 1, \pm 3\}$

$D(8) = \{x \in \mathbb{Z}^* ; x|8\} = \{\pm 1, \pm 2, \pm 4, \pm 8\}$

D(a) = D(–a).

Qualquer que seja o inteiro $a \neq 0$, se $x|a$, então $-a \leq x \leq a \Rightarrow D(a) \subset [-a, a]$ e isto significa que qualquer inteiro $a \neq 0$ tem um número finito de divisores.

Como a possui um número finito de divisores, podemos encontrar todos os divisores naturais de a. A primeira afirmação está enunciada na seguinte proposição.

Proposição 2: Se d e n são números inteiros tal que $d|n$ e $n \neq 0$, então $|d| \leq |n|$.

Demonstração: Da definição (2) temos que existe q inteiro tal que $n = d \cdot q$. Como $n \neq 0$ devemos ter $|q| \geq |1|$ e pela monotonia da relação de ordem, obtemos que $|n| = |d \cdot q| \geq |d|$.■

5.1 DIVISORES COMUNS DE DOIS INTEIROS

Definição 5. Chama-se divisor comum de dois inteiros a e b todo inteiro d ≠ 0 tal que d|a e d|b.

Iremos denotar o conjunto $D(a,b) = \{x \in \mathbb{Z}^* ; x|a \text{ e } x|b\} = \{x \in \mathbb{Z}^* ; x \in D(a) \text{ e } x \in D(b)\}$.

NOTA. $D(a,b) = D(a) \cap D(b)$.

A *interseção* (∩) é uma operação comutativa, de modo que D(a,b) não depende da ordem dos inteiros dados a e b, ou seja, D(a,b) = D(b,a).

Obs.: $D(a,b) \neq \emptyset$; $D(0,0) = \mathbb{Z}^*$.

Exemplo 3: Sejam os inteiros a = 18 e b = 20. Temos:

$D(18) = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18\}$

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

Assim:

$$D(18,20) = D(18) \cap D(20) = \{\pm 1, \pm 2\}$$

6 PRINCÍPIO DA BOA ORDENAÇÃO

Definição 6: Seja A um conjunto de inteiros. Chama-se elemento mínimo de A um elemento $a \in A$ tal que $a \leq x$ para todo $x \in A$.

O mínimo de A é indicado pela notação minA.

Teorema 4 (Princípio da Boa Ordem para $\mathbb{Z}$)**:** Todo conjunto não vazio A de inteiros não negativos possui o elemento mínimo.

$$(\forall\ A \subset \mathbb{Z}_+, A \neq \emptyset) \Rightarrow \exists\ \text{min}A$$

Demonstração: Veja [5].

Teorema 5 (*Algoritmo da Divisão*)**:** Se a e b são dois inteiros, com b > 0, então existem e são únicos os inteiros q e r que satisfazem às condições: $a = bq + r$ e $0 \leq r < b$.

Demonstração:

Existência

Seja S o conjunto de todos os inteiros não-negativos que são da forma $a - bx$, com $x \in \mathbb{Z}$, isto é:

$$S = \{a - bx\ ;\ x \in \mathbb{Z}\ ,\ a - bx \geq 0\}$$

Este conjunto S não é vazio ($S \neq \emptyset$), porque, sendo b > 0, temos $b \geq 1$ e, portanto, para $x = -|a|$, resulta:

$$a - bx = a + b\,|\,a\,| \geq a + |\,a\,| \geq 0$$

Assim sendo, pelo *Princípio da boa ordenação*, existe o *elemento mínimo* r de S tal que

$$0 \leq r \text{ e } r = a - bq \text{ ou } a = bq + r, \text{ com } q \in \mathbb{Z}$$

Além disso, temos $r < b$, pois, se fosse $r \geq b$, teríamos:

$$0 \leq r - b = a - bq - b = a - b(q + 1) < r$$

isto é, r não seria o *elemento mínimo* de S.

Unicidade

Para demonstrar a unicidade de q e r, suponhamos que existem dois outros inteiros q_1 e r_1 tais que

$$a = bq_1 + r_1 \text{ e } 0 \leq r_1 < b$$

Então, teremos:

$$bq_1 + r_1 = bq + r \Rightarrow r_1 - r = b(q - q_1) \Rightarrow b \mid (r_1 - r)$$

por outro lado, temos:

$$- b < r - r_1 < b,$$

isto é

$$| r_1 - r | < b$$

Assim, $b|(r_1 - r)$ e $| r_1 - r | < b$ e, portanto: $r_1 - r = 0$, e como $b \neq 0$, também temos $q - q1 \neq 0$. Logo, $r_1 = r$ e $q_1 = q$. ■

Corolário 1 (*Algoritmo da Divisão*)**:** Se a e b são dois inteiros com $b \neq 0$, existem e são únicos os inteiros q e r que satisfazem às condições: $a = bq + r$, $0 \leq r < | b |$

Demonstração:

De fato, se $b > 0$, nada há que demonstrar, e se $b < 0$, então $| b | > 0$, e por conseguinte existem e são únicos os inteiros q_1 e r tais que

$$a = |b|q1 + r \text{ e } 0 \leq r < |b|$$

ou seja, por ser $|b| = -b$:

$$a = b(-q_1) + r \text{ e } 0 \leq r < |b|$$

Logo, existem e são únicos os inteiros $q = -q_1$ e r tais que

$$a = bq + r \text{ e } 0 \leq r < |b|. \blacksquare$$

NOTA. Os inteiros a, b, q e r são denominados respectivamente o *dividendo*, o *divisor*, o *quociente* e o *resto* na divisão de a por b.

Agora, veremos alguns exemplos para melhor assimilar o teorema mencionado.

Exemplo 4: Determine o quociente *q* e o resto *r* na divisão de $a = 55$ por $b = -13$ que satisfazem às condições do *algoritmo da divisão*.

Solução: Realizando a divisão usual dos valores absolutos de *a* e *b*, teremos:

$$55 = 13 \cdot 4 + 3 \Longrightarrow 55 = (-13) \cdot (-4) + 3,$$

onde $0 \leq 3 < |-13|$. Logo, o quociente $q = -4$ e o resto $r = 3$.

Exemplo 5: Determine o resto da divisão de $a = -90$ e $b = -11$ que satisfazem às condições do *algoritmo da divisão*.

Solução: Realizando a divisão usual dos valores absolutos de *a* e *b*, teremos:

$$\begin{aligned} 90 = 11 \cdot 8 + 2 \Longrightarrow -90 &= -11 \cdot 8 - 2 \\ &= -11 \cdot 8 - 11 + 11 - 2 \\ &= -11 \cdot 9 + 9. \end{aligned}$$

Logo, o quociente $q = 9$ e o resto $r = 9$ satisfaz as condições do teorema.

7 CONJUNTO DOS MÚLTIPLOS DE UM INTEIRO

Definição 7: O conjunto de todos os múltiplos de um inteiro qualquer $a \neq 0$ é indicado por M(a), ou seja: $M(a) = \{x \in \mathbb{Z};\ a|x\} = \{aq;\ q \in \mathbb{Z}\}$

Assim, por exemplo:

$$M(-1) = M(1) = \mathbb{Z}$$

$$M(2) = \{2q;\ q \in \mathbb{Z}\} = \{0, 2, 4, 6, 8, ...\}$$

$$M(5) = \{5q;\ q \in \mathbb{Z}\} = \{0, 5, 10, 15, 20, ...\}$$

Para todo inteiro $a \neq 0$, se tem $M(a) = M(-a)$.

Pela definição (4) temos,

$$M(a) = \{aq;\ q \in \mathbb{Z}\}$$

$$M(-a) = \{-aq;\ q \in \mathbb{Z}\}.$$

O número a possui infinitos múltiplos, porém o zero é uma exceção. O zero é o único múltiplo de zero, pois qualquer número inteiro multiplicado por zero é igual a zero.

7.1 MÚLTIPLOS COMUNS DE DOIS INTEIROS

Definição 8: Sejam a e b dois inteiros diferentes de zero ($a \neq 0$ e $b \neq 0$). Chama-se múltiplo comum de a e b todo inteiro x tal que a|x e b|x. Ou seja, múltiplo comum de a e b é todo inteiro que pertence concomitantemente aos conjuntos M(a) e M(b).

O conjunto de todos os múltiplos comuns de a e b indica-se pela notação M(a,b).

$M(a,b) = \{x \in \mathbb{Z};\ a|x \text{ e } b|x\} = \{x \in \mathbb{Z};\ x \in M(a) \text{ e } x \in M(b)\}$

Portanto, $M(a,b) = M(a) \cap M(b)$

A *interseção* ($\cap$) é uma operação comutativa, de modo que M(a,b) não depende da ordem dos inteiros dados a e b, ou seja, M(a,b) = M(b,a).

Exemplo 6: Sejam os inteiros a = 8 e b = -12. Temos:

$$M(8) = \{8q|q \in \mathbb{Z}\} = \{0, 8, 16, 24, 32, 40, 48, 56, 72, 80, 88, 96, ...\}$$

$$M(-12) = \{-12q|q \in \mathbb{Z}\} = \{0, 12, 24, 36, 48, 60, 72, 84, 96, 108, ...\}$$

Assim:

$$M(8,-12) = M(8) \cap M(-12) = \{0, 24, 48, 72, 84, 96, ...\}$$

8 MDC DE DOIS INTEIROS

Definição 9: Sejam a e b inteiros diferentes de zero. O máximo divisor comum, entre a e b é o mesmo d que satisfaz as seguintes condições:

(1) d é um divisor comum de a e b, isto é, d|a e d|b;

(2) d é o maior inteiro positivo com a propriedade (1), isto é, se c|a e se c|b, então c|d.

O *máximo divisor comum* de a e b indica-se pela notação mdc(a,b).

Teorema 6: Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Um inteiro positivo d ($d > 0$) é o mdc(a,b) se e somente se satisfaz às condições:

(1) d | a e d | b

(2) se c | a e se c | b, então c | d

Demonstração:

(⇒) Suponhamos que o mdc (a,b) = d. Então, d|a e d|b, isto é, a condição (1) é satisfeita. Por outra parte, existem inteiros x e y tais que ax + by = d e, portanto, se c|a e se c|b, então c|(ax + by) e c|d, isto é, a condição (2) também é satisfeita.

(⇐) Reciprocamente, seja d um inteiro positivo qualquer que satisfaz às condições (1) e (2). Então, pela condição (2), todo divisor comum c de a e b também é divisor de d, isto é, c|d, e isto implica $c \leq d$. Logo, d é o mdc(a,b). ■

Observe que mdc(a,b) = mdc(b,a), além disso:

I. O mdc(0,0) não existe

II. O mdc(a,1) = 1

III. Se $a \neq 0$, então mdc(a,0) = | a |

IV. Se a|b, então mdc(a,b) = | a |

Exemplo 7: mdc(-5,1) = 1, mdc(–8,0) = | –8 | = 8

Exemplo 8: a = 48, b = 72

D(48) = {1, 2, 3, 4, 6, 8, 12, 16, 24, 48}

D(72) = {1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72}

D(48) ∩ D(72) = {1, 2, 3, 4, 6, 8, 12, 24} ⇒ mdc(48,72) = 24

Definição 10: Quando o MDC entre dois números for igual a 1 diremos que esses números são coprimos ou primos entre si, isto é, mdc(a,b) = 1. Assim, 8 e 15 são primos entre si. Para mais detalhes veja [6].

8.1 MDC DE VÁRIOS INTEIROS

Teorema 7: mdc(a,b,c) = mdc(mdc(a,b),c)

Demonstração:

Com efeito, seja mdc(a,b,c) = d e mdc(a,b) = e. Então, d|a, d|b e d|c, e como existem inteiros x e y tais que ax + by = e, segue-se que d|(ax + by) ou d|e, isto é, d é um *divisor comum* de e e c(d|e e d|c).

Por outra lado, se f é um *divisor comum* qualquer de e e c(f|e e f|c), então f|a, f|b e f|c, o que implica $f \leq d$.

Assim sendo, o mdc(e,c) = d, isto é, o mdc(mdc(a,b),c) = mdc(a,b,c). ■

9 MMC DE DOIS INTEIROS

Definição 11: Sejam a e b dois inteiros diferentes de zero ($a \neq 0$ e $b \neq 0$). Chama-se *mínimo múltiplo comum* de a e b o inteiro positivo m (m > 0) que satisfaz às condições:

(1) a|m e b|m

(2) se a|c e se b|c, com c > 0, então $m \leq c$.

Observe-se que, pela condição (1), m é um múltiplo comum de a e b, e pela condição (2), m é o *menor* dentre todos os múltiplos comuns positivos de a e b.

O mínimo múltiplo comum de a e b indica-se pela notação mmc(a,b).

Pelo Princípio da boa ordenação, o conjunto dos múltiplos comuns positivos de a e b possui o elemento mínimo e, portanto, o mmc(a,b) existe sempre e é único. Ademais, por ser o produto ab um múltiplo comum de a e b, segue-se que o $mmc(a,b) \leq |ab|$.

Em particular, se a|b, então o mmc(a,b) = | b |.

Exemplo 9:

$m_+(4) = \{4, 8, 12, 16, 20, 24, ...\}$

$m_+(6) = \{6, 12, 18, 24, 30, ...\}$

$m_+(4) \cap m_+(6) = \{12, 24, ...\} \Rightarrow mmc(4,6) = 12$

9.1 MMC DE VÁRIOS INTEIROS

Assim como podemos calcular o MDC de vários números, podemos estender também a noção de MMC para vários números, como faremos a seguir. No caso de três inteiros a, b e c, diferentes de zero, o mmc(a,b) é o inteiro positivo m (m > 0) que satisfaz às condições:

(1) a|m, b|m e c|m

(2) se a|e, se b|e e se c|e, com e > 0, então m ≤ e.

10 RELAÇÃO ENTRE O MDC E O MMC

Teorema 8: Para todo par de inteiros positivos a e b subsiste a relação:

$$mdc(a,b) \cdot mmc(a,b) = | ab |$$

Demonstração:

Seja mdc(a,b) = d e mmc(a,b) = m. Como a|a(b/d) e b|b(a/d), segue-se que ab/d é um múltiplo comum de a e b. Portanto, existe um inteiro positivo k tal que

$$ab/d = mk, k \in \mathbb{N}$$

o que implica:

$$a/d = (m/b)k \text{ e } b/d = (m/a)k$$

isto é, k é um *divisor comum* dos inteiros a/d e b/d. Mas, a/d e b/d são primos entre si, de modo que k = 1. Assim sendo, temos:

$$ab/d = m \text{ ou } ab = dm$$

isto é:

$$ab = mdc(a,b) \cdot mmc(a,b) \blacksquare$$

Com essa relação podemos determinar o mmc de dois inteiros quando se conhece o seu mdc, e vice-versa.

Exemplo 10: Sabendo que o produto entre dois números inteiros positivos é igual 15000 e o máximo divisor comum entre eles é 30. Qual o mínimo múltiplo comum desses dois números?

Solução: Pelo teorema (5) temos que: $mdc(a,b) \cdot mmc(a,b) = ab$. Substituindo os dados informados no enunciado da questão, temos que:

$$30 \cdot mmc(a,b) = 15000 \Rightarrow mmc(a,b) = 15000/30 = 500$$

Corolário 2: Para todo par de inteiros positivos a e b, o $mmc(a,b) = ab$ se, e somente se, o $mdc(a,b) = 1$

Demonstração:

($\Rightarrow$) Se o $mdc(a,b) = 1$, então:

$$ab = 1 \cdot mmc(a,b) = mmc(a,b)$$

($\Leftarrow$) Reciprocamente, se o $mmc(a,b) = ab$, então:

$$mdc(a,b) \cdot ab = ab \Rightarrow mdc(a,b) = 1\blacksquare$$

11 APLICAÇÕES DOS MÚLTIPLO E DOS DIVISORES

De posse do conhecimento de algumas definições, teoremas e corolários, agora apresentaremos algumas aplicações dos múltiplos e divisores.

Problema 6: Sendo a um inteiro qualquer, mostrar que $2|a(a + 1)$.

Solução: Se $a \in \mathbb{Z}$, então $a = 2k$ ou $a = 2k + 1$.

(I) $a = 2k \Rightarrow a(a + 1) = 2 \cdot \underbrace{k(2k + 1)}_{q} = 2q \Rightarrow 2|a(a + 1)$.

(II) $a = 2k + 1 \Rightarrow a(a + 1) = (2k + 1)(2k + 1 + 1) = (2k + 1)(2k + 2) = 2 \cdot \underbrace{(2k + 1)\ (k + 1)}_{q} = 2q$

$\Rightarrow 2|\ a(a + 1)$.

Problema 7: Sendo a um inteiro qualquer, mostrar que 3|a(a + 1)(a + 2).

Solução: Se a ∈ ℤ, então a = 3k; a = 3k + 1 ou a = 3k + 2.

i. $a = 3k \Rightarrow a(a+1)(a+2) = 3\cdot\underbrace{k(3k+1)(3k+2)}_{q} = 3q \Rightarrow 3|a(a+1)(a+2)$.

ii. $a = 3k+1 \Rightarrow a(a+1)(a+2) = (3k+1)(3k+1+1)(3k+1+2) = (3k+1)(3k+2)(3k+3) = 3\cdot\underbrace{(3k+1)(3k+2)(k+1)}_{q} = 3q \Rightarrow 3|a(a+1)(a+2)$.

iii. $a = 3k+2 \Rightarrow a(a+1)(a+2) = (3k+2)(3k+2+1)(3k+2+2) = (3k+2)(3k+3)(3k+4) = 3\cdot\underbrace{(3k+2)(k+1)(3k+4)}_{q} = 3q \Rightarrow 3|a(a+1)(a+2)$.

Assim, qualquer que seja a, 3|a(a + 1)(a + 2).

Problema 8: Demonstrar que $30|(n^5 - n)$.

Solução: Note que 30 = 2 · 3 · 5. Logo, se provarmos que 2, 3 e 5 dividem $(n^5 - n)$, o 30 também o dividirá.

$n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = n(n+1)(n-1)(n^2+1)$.

Caso (1): Conforme o problema 6, n(n + 1) é múltiplo de 2, ou seja, 2|n(n + 1).

Assim, $n(n+1)(n-1)(n^2+1)$ é múltiplo de 2.

Caso (2): Seja (n − 1) = (n − 3 + 2).

Fazendo n − 3 = n', temos (n − 3 + 2) = n' + 2, ou seja, conforme o problema 7, n(n + 1)(n − 1) é múltiplo de 3. Ou invertendo a ordem temos: (n − 1)n(n + 1) que é o produto de três números consecutivos.

Assim, $n(n+1)(n-1)(n^2+1)$ é múltiplo de 3.

Caso (3): Devemos provar que $n(n+1)(n-1)(n^2+1)$ é divisível por 5.

Se n ∈ ℤ, então n = 5k; n = 5k + 1; n = 5k + 2; n = 5k + 3 ou n = 5k + 4.

i. $n = 5k \Rightarrow n(n+1)(n-1)(n^2+1) = 5\cdot\underbrace{k(5k+1)(5k-1)[(5k)^2+1]}_{q} = 5q \Rightarrow$

$5 | n(n+1)(n-1)(n^2+1)$.

ii. $n = 5k+1 \Rightarrow n(n+1)(n-1)(n^2+1) = 5\cdot\underbrace{k(5k+1)(5k+2)[(5k+1)^2+1]}_{q} = 5q \Rightarrow$

$5 | n(n+1)(n-1)(n^2+1)$.

iii. $n = 5k+2 \Rightarrow n(n+1)(n-1)(n^2+1) = (5k+1)(5k+2)(5k+3)\underbrace{[(5k+2)^2+1]}_{5\cdot 5k^2+5\cdot 4k+5} =$

$5\cdot\underbrace{(5k+1)(5k+2)(5k+3)(5k^2+4k+1)}_{q} = 5q \Rightarrow 5 | n(n+1)(n-1)(n^2+1)$.

iv. $n = 5k + 3 \Rightarrow n(n + 1)(n - 1)(n^2 + 1) = (5k + 2)(5k + 3)(5k + 4)\underbrace{[(5k+3)^2 + 1]}_{5\cdot 5k^2 + 5\cdot 6k + 5\cdot 2} =$

$5\cdot\underbrace{(5k+2)(5k+3)(5k+4)(5k^2+6k+2)}_{q} = 5q \Rightarrow 5 \mid n(n + 1)(n - 1)(n^2 + 1).$

v. $n = 5k + 4 \Rightarrow n(n + 1)(n - 1)(n^2 + 1) = (5k + 3)(5k + 4)(5k + 5)[(5k + 4)^2 + 1] =$

$5\cdot\underbrace{(5k+1)(5k+3)(5k+4)[(5k+4)^2+1]}_{q} = 5q \Rightarrow 5 \mid n(n + 1)(n - 1)(n^2 + 1).$

Assim, qualquer que seja n, $5|n(n + 1)(n - 1)(n^2 + 1)$.

Pelos casos (1), (2) e (3). Logo, $30|(n^5 - n)$.

Problema 9: Na divisão do inteiro a = 427 por um inteiro positivo b o *quociente* é 12 e o *resto* é r. Achar o *divisor* b e o *resto* r.

Solução: Pelo Algoritmo da Divisão temos: $427 = 12b + r$.

Como 427 divido por 12 não é uma divisão exata temos: $427 = 12\cdot 35 + 7$, ou seja, b = 35 r = 7 é uma das soluções.

Obtemos outros valores para $a < 36$, pois $12 \cdot 36 = 432 > 427$.

Assim,

$427 = 12 \cdot 34 + 19$, com b = 34 e r = 19

$427 = 12 \cdot 33 + 31$, com b = 33 e r = 31

Como 427/32 é maior que 12, as únicas soluções são: b = 33 e r = 31; b = 34 e r = 19; b = 35 e r = 7.

A proposição apresentada a seguir é de grande utilidade na resolução de vários problemas em Teoria dos Números.

Proposição 3: Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a + b$ divide $a^{2n+1} + b^{2n+1}$.

Demonstração: Provaremos isto por indução sobre n.

i. P(1) é verdadeira, pois $a + b$ divide $a^3 + b^3 = (a + b)(a^2 - ab + b^2)$.

ii. Vamos admitir que P(k) é verdadeira, isto é, $(a + b)|(a^{2k+1} + b^{2k+1})$, para algum $k > 1$ com $k \in \mathbb{N}$.

iii. Vamos provar que P(k + 1) é verdadeira, ou seja, $(a + b)|(a^{2k+3} + b^{2k+3})$. Temos que:

$$\begin{aligned} a^{2k+3} + b^{2k+3} &= a^2a^{2k+1} + b^2b^{2k+1} \\ &= a^2a^{2k+1} + (b^2a^{2k+1} - b^2a^{2k+1}) + b^2b^{2k+1} \\ &= a^{2k+1}(a^2 - b^2) + b^2(a^{2k+1} + b^{2k+1}). \end{aligned}$$

Como $(a + b)|(a^2 - b^2) = (a + b)(a - b)$ e, por hipótese, $(a + b)|(a^{2k+1} + b^{2k+1})$, decorre da igualdade acima e do Teorema 1 item 7 que $(a + b)|(a^{2n+1} + b^{2n+1})$.

Vamos acompanhar uma solução de ([7], p. 23) para solucionarmos o problema 11.

Problema 10: Mostre que $14|3^{4n+2} + 5^{2n+1}$ para todo $n \in \mathbb{N}$.

Solução: Repare que:

$$\begin{aligned} 3^{4n+2} + 5^{2n+1} &= 3^{2(2n+1)} + 5^{2n+1} \\ &= 9^{2n+1} + 5^{2n+1}. \end{aligned}$$

Pela proposição anterior, temos que

$$(9 + 5) \mid 9^{2n+1} + 5^{2n+1}.$$

Portanto,

$$14|3^{4n+2} + 5^{2n+1}.$$

Problema 11: Prove que 5 divide $1^{99} + 2^{99} + 3^{99} + 4^{99} + 5^{99}$.

Solução: Dividimos $1^{99} + 2^{99} + 3^{99} + 4^{99} + 5^{99}$ em múltiplos de 5, assim:

i. $5 = (1 + 4) \mid 1^{99} + 4^{99}$

ii. $5 = (2 + 3) \mid 2^{99} + 3^{99}$

iii. $5 \mid 5^{99}$

Pela generalização do Teorema 1 item 7, temos que

$$5 \mid (1^{99} + 4^{99}) + (2^{99} + 3^{99}) + 5^{99}$$

Portanto, 5 divide $1^{99} + 2^{99} + 3^{99} + 4^{99} + 5^{99}$.

Problema 12: O número 446 foi dividido em duas parcelas, tais que a maior dividida pela menor deixa quociente 33 e resto 4. Qual a maior dessas parcelas?

Solução: De acordo com os dados fornecidos,

$$P_1 + P_2 = 446 \text{ (I)}$$

Pelo *Algoritmo da Divisão*

$$P_1 = P_2 \cdot 33 + 4 \text{ (II)}$$

Substituindo (II) em (I)

$$P_2 \cdot 33 + 4 + P_2 = 446 \Rightarrow P_2 = 13$$

Substituindo P_2 na equação (I)

$$P_1 + P_2 = 446 \Rightarrow P_1 = 433$$

Logo, a maior parcela é 433.

Agora utilizamos um exemplo prático do Algoritmo da Divisão na Criptografia RSA. Seguiremos o passo a passo conforme ([8], p.43). Assim, realizamos a pré-codificação que é a etapa que se convertem as letras em números, em seguida a codificação de uma mensagem e por fim a decodificação de uma mensagem.

12 CRIPTOGRAFIA

A criptografia é a ciência que estuda a forma de transmitir mensagens de forma segura, ou seja, apenas o emissor e o receptor são capazes de identificar o conteúdo da mensagem. Tem-se notícia de que persas, gregos e chineses utilizavam vários métodos para ocultar mensagens. A evolução da criptografia foi no sentido de não mais ocultar fisicamente as mensagens, mas usar estratégias para ocultar o seu significado às pessoas que não fossem as legítimas destinatárias das mesmas, de modo que pudessem ser veiculadas através de um canal público de comunicação.

Com o advento dos computadores e sua disseminação, houve a necessidade de buscar uma uniformização nos procedimentos. Há vários tipos de criptografia e um dos mais usados é o sistema RSA, que iremos apresentar aqui.

No RSA, a ideia básica é simples: dados dois números primos p e q, o seu produto é um número n. Esse número é a chave pública, enquanto p e q são as chaves privadas. Conhecidos p e q, é relativamente fácil achar n, pois basta multiplicar p por q, mas é difícil achar p e q a partir de n, pois este precisará ser fatorado e isso pode levar muito tempo.

12.1 PRÉ-CODIFICAÇÃO DE UMA MENSAGEM

A pré-codificação é a etapa em que se convertem as letras em números, ou seja, a mensagem original é convertida em uma sequência de números. Na tabela abaixo temos as letras do alfabeto e seus respectivos números que os representam.

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Tabela 1: Conversão de letras em números

Texto original: UESPI

Texto convertido em números: 3014282518

O processo final da pré-codificação consiste em dividir em blocos o número produzido ao converter o texto em número, evitando-se que o bloco comece por 0, pois pode ocorrer problema na decodificação: dado o bloco 024, por exemplo, ao decodificar pode ser que apareça apenas 24, gerando problema para obter o texto original. Para essa divisão é necessário escolher dois números primos distintos p e q e determinar n = pq. Como exemplo vamos escolher p = 3 e q = 11, logo n = 3 · 11 = 33. Os blocos deverão ser números menores que n, portanto poderão ser divididos da seguinte maneira: 30 – 14 – 28 – 25 – 18.

É importante ressaltar que a escolha dos blocos devem seguir a sequência do texto original, pois ao inverter a sequência pode ocorrer a decodificação de uma palavra diferente da original, por exemplo, mala e lama.

12.2 CODIFICAÇÃO DE UMA MENSAGEM

Para o processo de codificação é necessário o valor de n, com n = p · q, e de um número inteiro positivo e tal que mdc(e, (p – 1)(q – 1)) = 1.

Os valores de p e q são mantidos em segredo, mas os valores n e e são divulgados, pois são os números necessários para cifrar. A chave de codificação do sistema RSA é dada pelo par (n, e), denominado *chave pública*.

Seja b um bloco, então b é um inteiro positivo menor que n. Para determinar o bloco b codificado, denotado por C(b), é preciso calcular o resto da divisão de b^e por n.

Como escolhemos p = 3 e q = 11 temos:

$$(p - 1) \cdot (q - 1) = 2 \cdot 10 = 20.$$

Assim, escolhemos e = 7 para garantir o mdc(e, (p − 1)(q − 1)) = 1. Iremos fazer os cálculos para obter cada bloco codificado.

Bloco 30: Calcular o resto da divisão de 30^7 por 33.

$30^3 = 27000 = 33 \cdot 818 + 6$

$(30^3)^2 = (33 \cdot 818 + 6)^2$

$30^6 = 33 \cdot q + 6^2$

$30^6 = 33 \cdot q + 33 + 3$

$30^6 = 33 \cdot q_1 + 3$

$30^6 \cdot 30 = (33 \cdot q_1 + 3) \cdot 30$

$30^7 = 33 \cdot q_2 + 90$

$30^7 = 33 \cdot q_2 + 33 \cdot 2 + 24$

$30^7 = 33 \cdot q_3 + 24$

Logo, o bloco 30 codificado será 24.

Bloco 14: Calcular o resto da divisão de 14^7 por 33.

$14^3 = 2744 = 33 \cdot 83 + 5$

$(14^3)^2 = (33 \cdot 83 + 5)^2$

$14^6 = 33 \cdot r + 5^2$

$14^6 = 33 \cdot r + 25$

$14^6 \cdot 14 = (33 \cdot r_1 + 25) \cdot 14$

$14^7 = 33 \cdot r_2 + 350$

$14^7 = 33 \cdot r_2 + 33 \cdot 10 + 20$

$30^7 = 33 \cdot r_3 + 20$

Logo, o bloco 14 codificado será 20.

Bloco 28: Calcular o resto da divisão de 28^7 por 33.

$28^3 = 21952 = 33 \cdot 665 + 7$

$(28^3)^2 = (33 \cdot 665 + 7)^2$

$28^6 = 33 \cdot t + 7^2$

$28^6 = 33 \cdot t + 33 + 16$

$28^6 = 33 \cdot t_1 + 16$

$28^6 \cdot 28 = (33 \cdot t_1 + 16) \cdot 28$

$28^7 = 33 \cdot t_2 + 448$

$28^7 = 33 \cdot t_2 + 33 \cdot 13 + 19$

$28^7 = 33 \cdot t_3 + 19$

Logo, o bloco 28 codificado será 19.

Bloco 25: Calcular o resto da divisão de 25^7 por 33.

$25^3 = 15625 = 33 \cdot 473 + 16$

$(25^3)^2 = (33 \cdot 473 + 16)^2$

$25^6 = 33 \cdot p + 256$

$25^6 = 33 \cdot p + 33 \cdot 7 + 25$

$25^6 = 33 \cdot p_1 + 25$

$25^6 \cdot 25 = (33 \cdot p_1 + 25) \cdot 25$

$25^7 = 33 \cdot p_2 + 625$

$25^7 = 33 \cdot p_2 + 33 \cdot 18 + 31$

$25^7 = 33 \cdot p_3 + 31$

Logo, o bloco 25 codificado será 31.

Bloco 18: Calcular o resto da divisão de 18^7 por 33.

$18^3 = 5832 = 33 \cdot 176 + 24$

$(18^3)^2 = (33 \cdot 176 + 24)^2$

$18^6 = 33 \cdot s + 576$

$18^6 = 33 \cdot s + 33 \cdot 17 + 15$

$18^6 = 33 \cdot s_1 + 15$

$18^6 \cdot 18 = (33 \cdot s_1 + 15) \cdot 18$

$18^7 = 33 \cdot s_2 + 270$

$18^7 = 33 \cdot s_2 + 33 \cdot 8 + 6$

$18^7 = 33 \cdot s_3 + 6$

Logo, o bloco 18 codificado será 6.

Portanto, ao realizar todos os cálculos, codifica-se a mensagem e obtêm-se os blocos: 24 – 20 – 19 – 31 – 6.

12.3 DECODIFICAÇÃO DE UMA MENSAGEM

Para decodificar uma mensagem é necessário conhecer dois números: n e um inteiro d, tal que o resto da divisão de $e \cdot d$ por $(p - 1) \cdot (q - 1)$ seja 1, com $1 \leq d < (p - 1)(q - 1)$.

A chave de decodificação é dada pelo par (n, d), o valor d é denominado chave particular ou chave de decifragem. Sendo a um bloco da mensagem codificada, denotada por D(a) a conclusão do processo de decodificação, isto é, o bloco original, para encontrar D(a) é preciso calcular o resto da divisão de a^d por n.

Seguindo nosso exemplo, temos n = 33, e = 7 e $(p - 1)(q - 1) = 20$. Efetuando a divisão usual que satisfazem o algoritmo, deve-se escrever a seguinte igualdade:

$$7 \cdot d = 20 \cdot m + 1$$

$$d = \frac{14m + 6m + 1}{7} = 2m + \frac{6m + 1}{7}$$

O valor d é um número inteiro, então é necessário que o lado direito da igualdade seja um número inteiro, mas para isso $\frac{6m+1}{7}$ deve ser inteiro. Portanto, m = 1 satisfaz esta condição. Logo, d = 3.

Com o valor de d determinado, pelo Algoritmo da Divisão temos:

- **Bloco 24:** O resto da divisão de 24^3 por 33.

  $24^3 = 13824 = 33 \cdot 418 + 30$
- **Bloco 20:** O resto da divisão de 20^3 por 33.

  $20^3 = 8000 = 33 \cdot 242 + 14$
- **Bloco 19:** O resto da divisão de 19^3 por 33.

  $19^3 = 6859 = 33 \cdot 207 + 28$
- **Bloco 31:** O resto da divisão de 31^3 por 33.

  $31^3 = 29791 = 33 \cdot 902 + 25$
- **Bloco 6:** O resto da divisão de 6^3 por 33.

  $6^3 = 216 = 33 \cdot 6 + 18$

Assim, ao efetuar todos os cálculos têm-se os blocos decodificados: 30 – 14 – 28 – 25 – 18.

Ao juntar esses blocos e obter um único número “3014282518”, temos o texto original convertido em número, que, pela tabela de conversão, corresponde à palavra **UESPI**.

Para números primos pequenos facilmente realizamos os cálculos, porém para números primos grandes isso será uma tarefa impossível de realizar sem ajuda de um computador.

13 CONSIDERAÇÕES FINAIS

Os objetivos principais deste trabalho foram: propiciar aos alunos do Ensino Médio uma abordagem mais específica e prática da relação fundamental da divisão partindo dos múltiplos e divisores, ou seja, ser **múltiplo de** é o mesmo que ser **divisível por**. Bem como, mostrar que conteúdos matemáticos aparentemente inúteis podem vir a ter uma utilidade no nosso dia a dia. Esse mesmo exemplo poderá ser utilizado para fazer uma revisão de conteúdos abordados no Ensino Fundamental, por exemplo, potenciação e MDC.

> A BNCC da área de Matemática e suas Tecnologias propõe **a consolidação, a ampliação e o aprofundamento das aprendizagens essenciais** desenvolvidas no Ensino Fundamental. Para tanto, propõe colocar em jogo, de modo mais inter-relacionado, os conhecimentos já explorados na etapa anterior, a fim de possibilitar que os estudantes construam uma visão mais integrada da Matemática, ainda na perspectiva de sua aplicação à realidade. ([2], p. 529)

Assim, devemos possibilitar aos alunos a retomada dos múltiplos e divisores no Ensino Médio como um importante aliado na resolução de cálculos mais complexos e o seu papel em situações cotidianas, por exemplo, a Criptografia RSA.

REFERÊNCIAS

[1] GARBI, Gilberto. Como a matemática se tornou a rainha das ciências. **Revista do Professor de Matemática**, Ano 36, n. 96, p. 28-32, mai./ago. 2018.

[2] BRASIL. Ministério da Educação **Base Nacional Comum Curricular.** Brasília: MEC, 2018.

[3] BIANCHINI, Edwaldo. **Matemática Bianchini** (6º ano). 8. ed. São Paulo: Moderna, 2015.

[4] ALENCAR FILHO, Edgard de. **Teoria elementar dos números**. São Paulo: Nobel, 1981.

[5] FERREIRA, Jamil. **A construção dos números**. 3. ed. Rio de Janeiro: SBM, 2013.

[6] FONSECA, Rubens Vilhena. **Teoria dos números**. Belém: UEPA, 2011.

[7] FREITAS, Antônio Carlos Pereira de. **Teorema fundamental da aritmética e aplicações**. Dissertação (Mestrado Profissional em Matemática em rede Nacional) – Universidade da Integração Internacional da Lusofonia Afro-Brasileira, Redenção, 2023.

[8] QUEIROZ, Fabricia Auxiliadora. Criptografia RSA: uma abordagem para o ensino médio. **Revista do Professor de Matemática**, Ano 37, n. 98, p. 43-47, jan./abr. 2019.