UNIVERSIDADE ESTADUAL DA PARAÍBA

CENTRO DE CIÊNCIAS E TECNOLOGIA

DEPARTAMENTO DE MATEMÁTICA

CURSO DE LICENCIATURA EM MATEMÁTICA

ALGORITMO DA DIVISÃO SOBRE OS NÚMEROS INTEIROS

HIAGO DE SOUSA MARINHO SOARES

CAMPINA GRANDE

Novembro de 2017

HIAGO DE SOUSA MARINHO SOARES

ALGORITMO DA DIVISÃO SOBRE OS NÚMEROS INTEIROS

Trabalho Acadêmico Orientado apresentado ao curso de Licenciatura em Matemática do Departamento de Matemática do Centro de Ciências e Tecnologia da Universidade Estadual da Paraíba em cumprimento às exigências legais para obtenção do título de licenciado em Matemática.

Orientador: Dr. Vandenberg Lopes Vieira

CAMPINA GRANDE

Novembro de 2017

S676a Soares, Hiago de Sousa Marinho.
Algoritmo da divisão sobre os números inteiros [manuscrito] / Hiago de Sousa Marinho Soares. - 2017
49 p.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia, 2017.
"Orientação : Prof. Dr. Vandenberg Lopes Vieira, Coordenação do Curso de Matemática - CCT."

1. Números inteiros. 2. Números primos. 3. Algoritmo da divisão.

21. ed. CDD 512.72

HIAGO DE SOUSA MARINHO SOARES

ALGORITMO DA DIVISÃO SOBRE OS NÚMEROS INTEIROS

Trabalho Acadêmico Orientado apresentado ao curso de Licenciatura em Matemática do Departamento de Matemática do Centro de Ciências e Tecnologia da Universidade Estadual da Paraíba em cumprimento às exigências legais para obtenção do título de licenciado em Matemática.

Aprovado em: 06 / Novembro / 2017

COMISSÃO EXAMINADORA

Prof. Dr. Vandenberg Lopes Vieira
Dpto. Matemática - CCT/UEPB
ORIENTADOR

Prof. Ms. Weiller Pelipe Chaves Barboza
Dpto. Matemática - CCT/UEPB
EXAMINADOR

Prof. Wallace Ferreira Gomes
Dpto. Matemática - CCT/UEPB
EXAMINADOR

Dedicatória

A toda minha família, em especial aos meus pais por todo incentivo e o Shalom.

Agradecimentos

Agradeço primeiramente Aquele que me gerou e me criou que é Senhor e sentido da minha vida, Deus, pois sem Ele nada poderia ter feito, Também sou grato pela a intercessão dos Santos e da Virgem de Guadalupe, á São Tomás de Aquino que me livrou de qualquer distração que ocorreu na elaboração desse trabalho, ao Beato Píer Jorge de Frassati, e Virgem de Guadalupe que sempre esteve ao meu lado, não desistindo de mim e dando forças para prosseguir e vencer todas as dificuldades que surgiram na vida acadêmica.

Aos meus familiares, de modo especial ao meu pai José Marconio e minha mãe Joventina de Sousa, que me deram amor, carinho e educaram conforme a vontade de Deus, e propiciando essa etapa da minha vida, sou grato por cada palavra, cada conselho, cada preocupação, por nunca desistirem de mim, e por esse exemplo de pai e mãe para mim. E também agradeço a meu irmão Heriverton que tanto me aconselhou e ajudou algumas vezes, principalmente no momento que estava a ponto de desistir, você foi instrumento de Deus na minha vida. Também agradeço a Priscylla Martins, minha namorada, que aguentou meus estresses, minha preguiça, meus desabafos, minha crises de estudo, e como Heriverton, ela aconselhou, rezou por mim e não permitiu que enfrentasse as dificuldades sozinhas, na medida do possível esteve ali do meu lado.

Um agradecimento muito especial ao meu orientador, professor Dr. Vandenberg Lopes, que generosamente se dispôs a orientar este trabalho com dicas enriquecedoras, não só neste, mas principalmente na vida acadêmica, você foi como um pai para mim. E de forma geral, agradeço a todos os professores do departamento de Matemática e a todos os docentes que foram testemunhas para hoje esta finalizando essa etapa da minha vida.

Por fim, agradeço a minha família Shalom que tanto contribui direta ou indiretamente, para realização desse momento, de maneira particular meus formadores: Nayara Messias, Lucas Vinicius e Luciana Mariano, e também ao meu amigo Lucas Siebra e por todos que intercederam por me, muito obrigado.

“Enquanto o amor humano tende a apossa-o do bem que encontra no seu objeto, o amor Divino cria o bem na criatura amada” (São Tomás de Aquino).

"Viver de amor é dar sem medida, Sem na terra o salário reclamar; Ah! Sem conta vou dando, convencida. Que, quem ama, não sabe calcular." (Santa Terezinha do Menino Jesus).

Resumo

O objetivo principal deste trabalho e apresentar o algoritmo da divisão no conjunto dos números inteiros, bem como, alguns exemplos que são resultados básicos para suas aplicações. Na qual, têm-se suma importância na Teoria Elementar dos Números. Para tanto, foram apresentados alguns resultados elementares sobre os números inteiros, como a sua fundamentação axiomática, o máximo divisor comum, mínimo múltiplo comum e números primos. Dentre estes, daremos enfasê ao Algoritmo da Divisão (Divisão Euclidiana), cujo resultados é bastante conhecido entre os leitores.

Palavras-chave: Números inteiros, Algoritmo da Divisão, Números Primos.

Abstract

The main objective of this paper is to present the division algorithm in the set of integers as well as some examples are basic documents for its applications. In which, there is a sum of importance in the Elementary Theory of Numbers. For this purpose, we have presented some elementary results on the integers, such as their axiomatic basis, the maximum common divisor, minimum common multiple and prime numbers. Among these, we will emphasize the Algorithm of the Division (Euclidean Division), whose result is well known among readers.

Keywords: Whole numbers, Division algorithm, Prime numbers.

Sumário

Introdução

A Teoria dos Números é um dos principais tópicos da matemática pura. Essencialmente, ela se dedica ao estudo dos números inteiros e de suas generalizações, tais como os inteiros algébricos. Hoje em dia, a Teoria dos Números não se destaca apenas pelos seus famosos problemas, tanto os abertos como os já solucionados. Como já se sabe, ela é importante para o nosso dia a dia. Com efeitos, aplicações em diversas áreas tais como Física, Química, Acústica, Computação e Criptografia, fazem dela um ramo especial, que desperta interesse não apenas para os matemáticos, mas também de pesquisadores de outras áreas.

Dentre os vários ramos da Teoria dos Números, três se têm destaque especial: A Teoria Algébrica, Teoria Analítica e a Teoria Elementar. Isto significa que é possível observar o estudo dos números inteiros sob ao menos três pontos de vista diferentes.

A Teoria Algébrica se dedica ao estudo dos números algébricos, ou seja, aqueles números complexos que são raízes de polinômios não nulos com coeficientes racionais, como por exemplo, o número $\alpha = \sqrt{3}/2$, que é raiz do polinômio $f(X) = 2X - \sqrt{3}$. Em especial, o conjunto dos inteiros algébricos, ou seja, o conjunto dos números algébricos que são raízes de polinômios mônicos com coeficientes inteiros, tem destaque especial. Com suas propriedades, muitos resultados foram obtidos, não apenas na Teoria dos Números, mas também na Álgebra Abstrata. Já a Teoria Analítica se dedica ao estudo mais avançados sobre os números primos. Ela emprega resultados da análise matemática, tanto real quanto complexa. Por fim, a Teoria Elementar se constitui basicamente no primeiro contato do estudante com as propriedades dos números inteiros. Os conceitos de divisibilidade, congruência entre inteiros e de números primos são à base do estudo inicial. E são esses tópicos que iremos abordar ao longo do trabalho.

Um dos resultados mais importantes e provados da matemática é o emblemático Teorema de Fermat. Pierre de Fermat foi matemático amador francês que dedicou a uma parte de seus

estudos à Teoria dos Números. E grande marco dele é a equação pitagórica, ou seja, a equação não linear,

$$x^2 + y^2 = z^2$$

que conhecemos no ensino basico de Teorema de Pitagóras, onde a soma dos quadrados dos catetos é igual a hipotenusa ao quadrado. Essa inspirou para adotar novas ideias na aritmética, tomando assim *O Últimо Teorema de Fermat.*

Neste trabalho, consideramos alguns resultados básicos da Teoria Elemetar dos Números, dando ênfase ao Algoritmo da Divisão (Divisão Euclidiana), o qual é um dos mais básicos e principais resultados da Teoria dos Números e diante disso, nosso estudo resultou do embasamento teórico sobre o tema, tendo como principal referência o livro de Prof. Dr. Vandenberg, "Um Curso Básico em Teoria dos Números". Assim, após apresentado estes conteúdos, concluímos com as aplicações os sistemas de númeração,o Algoritmo de Euclides e por fim o crivo de Erástotenes, resultados fundamentais para estudos da propriedades algébricas dos números inteiros que são apresentadas no ensino fundamental de uma forma mais simples, faremos com abordagem mais formal.

Capítulo 1

Números Inteiros

Neste capítulo, iremos abordar um pouco sobre os números inteiros, esse conjunto que é fundamental no ramo da Matemática, e seus subtemas será a fundamentaçao axiomática dos inteiros. A *divisibilidade* nos conjuntos dos números inteiros e suas propriedades, o máximo divisor comum e mínimo múltiplo comum que estão relacionados como resultados elementares, entretanto, serão necessários para os capítulos seguintes. E ainda daremos ênfase ao Algoritmo da Divisão (Divisão Euclidiana), pois é um resultado fundamental na Teoria dos Números.

1.1 Uma Fundamentação Axiomática dos Inteiros

As propriedades a seguir são pré-requisitos dos próximos resultados e base de fundamentação teórica do assunto central desse trabalho.

Inicialmente, denotemos o conjunto dos números inteiros pela representação usual:

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}.$$

As propriedades das operações de adição e multiplicação de números inteiros serão consideradas axiomas, pois não iremos prová-las aqui.

A operação de adição de números inteiros, indicada por " + ", satisfaz os seguintes axiomas:

A_1 **Associatividade da adição:** Para inteiros a, b e c, temos

$$a + (b + c) = (a + b) + c.$$

A_2 **Comutatividade da adição:** Dados inteiros a e b,

$$a + b = b + a.$$

A_3 **Existência de elemento neutro para a adição:** Existe um único elemento $0 \in \mathbb{Z}$, chamado **zero**, de maneira que,

$$a + 0 = a, \quad \forall\ a \in \mathbb{Z}.$$

A_4 **Existência de inverso aditivo:** Dado um inteiro a, existe um único inteiro $-a$, chamado **simétrico** ou **oposto** de a, tal que,

$$a + (-a) = 0.$$

A multiplicação é associativa, comutativa e tem elemento neutro (o número 1), assim como a adição. Denotaremos a multiplicação por "$\cdot$",

M_1. **Associatividade da multiplicação:** Para quaisquer inteiros a, b e c,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

M_2. **Comutatividade da multiplicação:** Dados inteiros a e b,

$$a \cdot b = b \cdot a.$$

M_3. **Existência de elemento neutro para multiplicação:** Existe um único elemento $1 \in \mathbb{Z}$, chamado **um**, tal que,

$$1 \cdot a = a, \quad \forall\ a \in \mathbb{Z}. \tag{1.1}$$

Para próximo axioma, usamos as duas operações, isto é,

M_4. **A multiplicação é distributiva em relação à adição:** Para todos a, b e $c \in \mathbb{Z}$, temos que

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

e por fim,

M_5. **Lei do cancelamento da multiplicação:** Dados inteiros a, b e c, com $a \neq 0$,

$$a \cdot b = a \cdot c \Rightarrow b = c.$$

A seguir vamos apresentar as propriedades que decorrem das anteriores.

Proposição 1.1. *Sejam a, b e c inteiros quaisquer. Então:*

(1) $a \cdot 0 = 0$.

(2) *Se $a + b = a + c$, então $b = c$.* ***(Propriedade cancelativa da adição)***

(3) *Se $a \cdot b = 0$, então $a = 0$ ou $b = 0$.* ***(Integridade de $\mathbb{Z}$)***

Demonstração: (1) Seja $a \in \mathbb{Z}$. Temos que

$$a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 = a \cdot 0 + 0, \tag{1.2}$$

Desse modo, $a \cdot 0 + a \cdot 0 = a \cdot 0$. E como $a \cdot 0 \in \mathbb{Z}$, então existe $-(a \cdot 0) \in \mathbb{Z}$ tal que $-(a \cdot 0) + (a \cdot 0) = 0$. Logo, adicionando $-(a \cdot 0)$ em ambos os membros de 1.2, e usando a propriedade associativa da adição, obtemos

$$(-(a \cdot 0) + a \cdot 0) + a \cdot 0 = -(a \cdot 0) + a \cdot 0,$$

ou seja, $0 + a \cdot 0 = 0$, desse modo concluímos que $a \cdot 0 = 0$.

(2) Queremos mostrar que $a + b = a + c$, onde $b = c$ (h), para isso vamos adicionar $-a$ em ambos os membros de (h)

$$-a + (a + b) = -a + (a + c) \Rightarrow (-a + a) + b = (-a + a) + c.$$

Logo, $0 + b = 0 + c$,isto é, $b = c$.

(3) Pelo item (1), obtemos que $a \cdot 0 = 0$, como hipótese temos que, $a \cdot b = 0$; daí segue-se que, $a \cdot b = a \cdot 0$. Se $a = 0$, o resultado segue naturalmente. Caso contrário, podemos usar a lei do cancelamento da multiplicação, temos que $b = 0$. □

A proposição seguinte nos recordar algo que aprendemos no ensino básico sobre os inteiros. As propriedades são conhecidas como as regras dos sinais, que são úteis para provar outras propriedades básicas dos inteiros.

Proposição 1.2 (**Regra dos Sinais**). *Se a e b são inteiros quaisquer, então*

(1) $-(-a) = a$.

(2) $(-a)\cdot(b) = -(a\cdot b) = a\cdot(-b)$.

(3) $(-a)\cdot(-b) = a\cdot b$.

Demonstração: (1) Note que por definição, se $a+b=0$, então $a=-b$. Por isso, como $a+(-a)=0$, segue imediato que $a=-(-a)$.

(2) Temos que

$$a\cdot b+(-a)\cdot(b) = (a+(-a))\cdot b = 0\cdot b = 0,$$

isto é, $(-a)\cdot(b) = -(a\cdot b)$. Da mesma maneira,

$$a\cdot b+a\cdot(-b) = a\cdot(b+(-b)) = a\cdot 0 = 0,$$

ou seja, $a\cdot(-b) = -(a\cdot b)$. Portanto,

$$(-a)\cdot(b) = -(a\cdot b) = a\cdot(-b).$$

(3) Usando inicialmente o item (2),

$$(-a)\cdot(-b) = -(a\cdot(-b)) = -(-(a\cdot b)),$$

agora, pelo item (1), $-(-a)=a$. Assim, $(-a)\cdot(-b) = a\cdot b$. □

No conjunto $\mathbb{Z}$ também está definida uma relação de ordem, chamada por "menor ou igual", denotada por " $\leqslant$ ". Para essa relação existe três propridades importantes são elas:

Propriedade Reflexiva: Para todo a, note que $a\leqslant a$.

Propriedade Anti-simétrica: Seja os inteiros a e b, se $a\leqslant b$ e $b\leqslant a$, então $a=b$.

Propriedade transitiva: Dados inteiros a, b e c, se $a\leqslant b$ e $b\leqslant c$, então $a\leqslant c$.

1.2 Divisibilidade em $\mathbb{Z}$

Nesta seção, vamos apresentar o conceito de divisibilidade no conjunto dos números inteiros e suas principais propriedades. Para evitar repetições de certas frases, vamos sempre considerar as letras a, b, c, e assim por diante, para indicar os números inteiros.

Definição 1.1. *Seja a e b dois números inteiros com, $b \neq 0$. Dizemos que b* ***divide*** *a, e indicamos por $b \mid a$, se existir $q \in \mathbb{Z}$ tal que*

$$a = bq. \tag{1.3}$$

Dessa forma,

$$b \mid a \;\Leftrightarrow\; a = bq \;\text{ para algum }\; q \in \mathbb{Z}.$$

Indicaremos o fato de b não divide a pelo símbolo $b \nmid a$.

Exemplo: Temos que $7 \mid 49$, $-3 \mid 21$, pois, $49 = 7 \cdot 7$, $21 = (-3) \cdot (-7)$ respectivamente, além disso note que $3 \nmid 49$, pois não existe $q \in \mathbb{Z}$, tal que $49 = 3 \cdot q$.

Notemos que $1 \mid a$, $a \mid a$ e $a \mid 0$ para qualquer inteiro a, pois

$$a = 1 \cdot a, \quad a = a \cdot 1 \quad \text{e} \quad 0 = a \cdot 0.$$

Notemos que $a \mid 0 \Leftrightarrow a = 0$. Portanto, excluímos o caso que 0 é divisor. △

A seguir enunciaremos alguns resultados que são propriedades elementares da divisibilidade, a qual suas demonstrações serão encontradas em [1].

Proposição 1.3. *Em $\mathbb{Z}$ valem, as seguintes propriedades:*

(1) $a \mid 0, \quad 1 \mid a \quad e \quad a \mid a, \quad com\ a \neq 0.$

(2) *Os únicos divisores de* 1 *são* 1 *e* -1.

(3) *Se* $a \mid b$ *e* $b \mid a$, *então* $a = \pm b$.

No teorema a seguir, veremos outras propriedades elementares da divisibilidade.

Teorema 1.1. *Dados $a, b, c, d \in \mathbb{Z}$, são válidas as seguintes propriedades:*

(1) *Se* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.

(2) *Se* $a \mid b$ *e* $c \mid d$, *então* $ac \mid bd$.

(3) *Se* $a \mid b$ *e* $a \mid c$, *então* $a \mid (mb + nc)$, $\forall m, n \in \mathbb{Z}$.

1.3 Divisão Euclidiana

O algoritmo da divisão (Divisão Euclidiana) é considerado um dos fundamentos da Teoria dos Números. Sendo bastante conhecido no ensino fundamental, porém é apresentado de uma maneira mais direta afim de tornar-se mais compreensível para os alunos. A divisão euclidiana é um resultado que servirá de base para propriedades algébricas nos números inteiros. Como já foi abordado às primeiras introduções da divisão no ensino fundamental são apresentadas com a forma de fácil de compreensão para os alunos e neste trabalho, vamos abordar com um nível mais formal da divisão euclidiana. Vejamos o seguinte teorema.

Teorema 1.2 (Divisão Euclidiana)**.** *Sejam $a, b \in \mathbb{Z}$, com $b > 0$. Então, existe únicos $q, r \in \mathbb{Z}$, respectivamente, tais que*

$$a = bq + r, \quad com \quad 0 \leq r < b. \tag{1.4}$$

Demonstração: Consideremos o conjunto

$$L = \{a - bq : q \in \mathbb{Z} \quad \text{e} \quad a - bq \geqslant 0\}.$$

Primeiramente, vamos verificar se L não é vazio. De fato, visto que $b \geqslant 1$, então $|a| \cdot b \geqslant |a|$. Logo,

$$a - (-|a|) \cdot b = a + |a| \cdot b \geqslant a + |a| \geqslant 0.$$

Como $x = a - (-|a|) \cdot b$ é da forma $a - bq$, com $q = -|a|$, segue que $x \in L$.

Mostremos agora a existência e a unicidade dos inteiros q e r.

(**Existência**) Sendo L limitado inferiormente (por zero, por exemplo) e não vazio, temos pelo Principio da Boa Ordenação (PBO), podemos encontrar este conceito em [5], que L possui menor elemento, digamos $r = \min L$.

Como $r \in L$, então $\quad r \geqslant 0$ e

$$r = a - bq, \quad \text{com} \quad q \in \mathbb{Z},$$

afirmamos que $r < b$. De fato, se isso não ocorre, então $r - b \geqslant 0$ e

$$r - b = a - bq - b = a - b(q + 1).$$

Portanto, $r - b \in L$ e $r - b < r$, o que contraria a minimalidade de r. Por consequência $a = qb + r$, com $q \in \mathbb{Z}$ e $0 \leqslant r < b$, isso mostra que existem os inteiros q e r.

(**Unicidade)** Para unicidade, consideremos $q_1, r_1 \in \mathbb{Z}$ tais que

$$a = bq_1 + r_1, \quad \text{com} \quad 0 \leqslant r_1 < b.$$

dessa forma, $bq + r = bq_1 + r_1$, o que resulta em

$$r - r_1 = b\,(q_1 - q)\,,$$

isto é, $b \mid (r - r_1)$. Como $|r - r_1| < b$, segue que $r - r_1 = 0$, ou seja, $r = r_1$. Portanto $q_1 = q$, visto que $b \neq 0$. □

Podemos generalizar a Divisão Euclidiana por meio da substituição na condição $b > 0$ por $b \neq 0$, conforme o seguinte resultado, que sua demonstração encontra-se em [2].

Corolário 1.1. *Se a e b são inteiros, com $b \neq 0$, então, existe únicos q e r tais que*

$$a = bq + r, \quad com \quad 0 \leq r < |b|\,. \tag{1.5}$$

Demonstração: É suficiente considerar o caso $b < 0$. O teorema anterior nos mostra que existem únicos inteiros q e r tais que,

$$a = |b|\,q_1 + r, \quad \text{com} \quad 0 \leq r < |b|\,.$$

Como $|b| = -b$, então,

$$a = |b|\,q_1 + r = b\,(-q_1) + r,$$

de maneira que, tomando $q = -q_1$, temos que,

$$a = bq + r, \quad \text{com} \quad 0 \leq r < |b|\,.$$

□

Os inteiros q e r dados em 1.5 são chamados, respectivamente, de **quociente** e **resto** da Divisão Euclidiana de a por b, respectivamente. Notemos que na Divisão Eucliadiana , com $a = bq + r$,

$$r = 0 \Leftrightarrow b \mid a.$$

Ora,

Observação 1.1. *Temos os seguintes casos particulares:*

- Se $a = 0$, então $q = r = 0$.
- Se $a > 0$ e $a < b$, $q = 0$ e $r = a$.

Exemplo: Determinar o quociente e o resto da Divisão Euclidiana de a por b quando:

a) $a = 65$ e $b = 6$

b) $a = -32$ e $b = 3$

c) $a = -2435$ e $b = -8$

Solução: (a) Como $65 = 10.6 + 5$ e $5 < 6$, então $q = 10$ e $r = 5$.

(b) Para este caso, vamos efetuar a divisão natural de 32 por 3. A seguir, manipularmos a expressão de modo conveniente. Se $32 = 10 \cdot 3 + 2$, então

$$\begin{aligned} -32 &= -10 \cdot 3 - 2 \\ &= -10 \cdot 3 - 2 + 3 - 3 \\ &= -10 \cdot 3 - 3 - 2 + 3 \\ &= 3 \cdot (-10 - 1) + 1 \\ &= 3 \cdot (-11) + 1. \end{aligned}$$

Assim, $q = -11$ e $r = 1$.

(c) Seja $a = -2435$ e $b = -8$, vamos efetuar a divisão natural de 2435 por 8 e usamos o artificio análogo ao caso b). Como $2435 = 304 \cdot 8 + 3$, temos:

$$\begin{aligned} -2435 &= 304\,(-8) - 3 \\ &= 304\,(-8) - 3 + 8 - 8 \\ &= 304\,(-8) - 8 - 3 + 8 \\ &= -8 \cdot (304 + 1) + 5 \\ &= -8 \cdot 305 + 5. \end{aligned}$$

Logo, $q - 305$ e $r = 5$. $\triangle$

Conforme a Divisão Euclidiana, se a é um numero inteiro qualquer, então a resolução da sua divisão por $b = 2$, obtemos os possíveis restos $r = 0$ ou $r = 1$, isto é,

$$a = 2q + r, \qquad \text{com } 0 \leqslant r < 1.$$

Se $r = 0$, então a é denotado da seguinte forma $a = 2q$ e é denominado **número par**; se $r = 1$, segue que a é da maneira $a = 2q + 1$ e é chamado de **número impar.**

Por exemplo, os números 8 e -16 são pares, pois

$$8 = 2 \cdot 4 \quad \text{e} \quad -16 = (-2) \cdot 8,$$

No entanto, 21 e -13 são impares, note que

$$21 = 4 \cdot 5 + 1 \quad \text{e} \quad -13 = 7 \cdot (-2) + 1.$$

Definição 1.2. *Pela **paridade** de um inteiro, queremos dizer se ele é par ou ímpar.*

Se P e I é denominado os conjuntos dos números pares e ímpares, respectivamente, então,

$$P = \{2k : k \in \mathbb{Z}\} \qquad \text{e} \qquad I = \{2k + 1; k \in \mathbb{Z}\}.$$

É imediato verificar que:

(1) $P \cap I = \emptyset$.

(2) Se $x, y \in P$, então $x \pm y \in P$ e $x \cdot y \in P$.

(3) Se $x, y \in I$, então $x \pm y \in P$ e $x \cdot y \in I$.

(4) Se $x \in P$ e $y \in I$, então $x \pm y \in I$ e $x \cdot y \in P$.

No capítulo 3 apresentaremos algumas aplicações da Divisão Euclidiana. Lembrando que um inteiro a é um quadrado perfeito quando $a = q^2$ para algum inteiro q.

1.4 Máximo Divisor Comum

O conceito de *máximo divisor comum* (mdc) é um dos conceitos primordiais da Teoria Elementar dos Números. Aqui vamos considerá-lo e apresentar algumas propriedades básicas.

No ensino básico o cálculo de mdc entre dois inteiros é, em geral, realizado por duas formas: através da fatoração canônica; e por meio dos conjuntos dos divisores positivos escolhendo, neste caso, o maior inteiro da interseção desses conjuntos.

Vale aqui chamar a atenção que tais métodos não são eficientes, mesmo para números grandes ao efetuarmos o mdc, pois dependendo dos valores dos inteiros, o cálculo do mdc entre

eles é no mínimo tedioso. De fato, determinar a fatoração canônica entre inteiros é um problema sem solução satisfatória, e como determinar todos os divisores positivos de um dado inteiro está instrinsecamente ligado à obtenção de fatoração canônica, então o segundo método também tem suas limitações. Por isso, no ensino básico considera-se sempre números relativamentes pequenos. Por exemplo, para calcularmos o mdc entre 22 e 64, iniciamos a divisão pelo menor primo que divide ao menos um deles. Fazendo isso, temos:

22,64	2
11,32	2
11,16	2
11,8	2
11,4	2
11,2	2
11,1	11
1,1	

Logo, considerando o produto dos fatores comuns, podemos concluir que o máximo divisor comum de 22 e 64 é 22.

O método mais eficiente para se determinar o máximo divisor comum entre dois inteiros é através do algoritmo de Euclides, o qual consiste em divisões sucessivas, tendo como base o Algoritmo da Divisão.

Numa linguagem mais técnica, podemos mostrar a existência de mdc entre quaisquer dois inteiros a e b com $a \neq 0$ ou $b \neq 0$ da seguinte forma. Sejam

$$D_a = \{n \in \mathbb{N} : n \mid a\} \quad e \quad D_b = \{n \in \mathbb{N} : n \mid b\},$$

em que $\mathbb{N}$ indica o conjunto dos naturais (ou inteiros positivos). É claro que $D_a \cap D_b \neq \emptyset$, pois $1 \mid a$ e $1 \mid b$. Assim, $D_a \cap D_b$ é um conjunto finito e, por isso, possui maior elemento, o qual é chamado **máximo divisor comum** de a e b.

Quando $a = b = 0$, os conjuntos D_a e D_b são infinitos. É por isso que este caso não será considerado e convencionaremos que o máximo divisor comum entre eles é zero.

O que iremos apresentar aqui é essencialmente a mesma coisa, mas usando certo rigor matemático e **destacando propriedades referentes ao conteúdo que tem como forma um dos pilares da aritmética de Euclides.**

Definição 1.3. *Dados $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$, o inteiro positivo d é o* ***máximo divisor comum*** *(mdc) de a e b, quando:*

(a) $d \mid a$ e $d \mid b$.

(b) Se $c \in \mathbb{Z}$, é um divisor comum de a e b, então c divide d.

Assim, o máximo divisor comum de a e b é um inteiro positivo que os divide e é divisível por todo divisor comum de a e b. Indicaremos este número por

$$d = mdc(a, b).$$

A notação utilizada pela maioria dos livros didáticos do ensino fundamental é $d = (a, b)$, isso é feito devido à praticidade. Notemos que:

$$mdc(a, b) = mdc(b, a).$$

Para alguns casos particulares, é trivial calcular o mdc. Por exemplo, se a é um número inteiro não nulo, temos claramente que:

(1) $mdc(a, 0) = |a|$.

(2) $mdc(a, 1) = 1$.

(3) $mdc(a, a) = |a|$.

Assim, para todo $b \in \mathbb{Z}$, temos que a divide b se, e somente se, $|a|$ é o mdc entre a e b, isto é,

$$a \mid b \;\Leftrightarrow\; mdc(a, b) = |a|.$$

Além disso, como $D_a = D_{(a)}$, então:

$$mdc(a, b) = mdc(-a, b) = mdc(a, -b) = mdc(-a, -b).$$

Desse modo, assumimos que a e b são sempre positivos.

O Teorema a seguir é fundamental para resoluções de muitos problemas na Teoria dos Números, pois tem uma importante identidade que relaciona os números a e b e seu mdc. Esta identidade é conhecida como identidade de **Bachet-Bézout**, o nome associado aos matemáticos franceses Étienne Bézout e Claude-Gaspard Bachet de Méziria que foram os primeiros a demonstrar a identidade, respectivamente, através do resultado para polinômios e para os números inteiros.

Teorema 1.3 (Identidade Bachet-Bézout). *Se $d = mdc(a, b)$, existem inteiros x_0 e y_0 tais que*

$$d = ax_0 + by_0.$$

Demonstração: Consideremos o conjunto:

$$X = \{ax + by : x, y \in \mathbb{Z} \quad \text{e} \quad ax + by > 0\}.$$

Note que, existem em X elementos que são estritamente positivos, por exemplo para $x = y = 1$, obtemos

$$a \cdot 1 + b \cdot 1 = a + b > 0 \Longrightarrow a + b \in X.$$

Admitindo H como o subconjunto de X constituindo por esses elementos. Desse modo, pelo PBO, H possui menor elemento d. Iremos mostrar que $d = mdc\,(a, b)$, sabendo que $d \in H$, existem $x_o, y_o \in \mathbb{Z}$ tais que

$$d = ax_o + by_o.$$

Usando o algoritmo da divisão com os elementos a e d, temos:

$$a = dq + r, \quad \text{com} \quad 0 \leqslant r < d, \tag{1.6}$$

isolando r substituindo o valor de d em 1.6, segue-se que

$$\begin{aligned} r \;=\; a - dq \;&=\; a - (ax_o + by_o) \cdot q \\ &=\; a - ax_o q - by_o q \\ &=\; a\,(1 - qx_o) + b\,(-qy_o)\,. \end{aligned}$$

Logo,

$$r = a\,(1 - qx_o) + b\,(-qy_o)\,.$$

Por isso, se $r \neq 0$, então $r \in H$. Mas, sendo $r < d$ então pela minimalidade de d, devemos necessariamente ter $r = 0$, isto é, $a = dq$, o que mostra que $d \mid a$.Por conseguinte mostra-se que $d \mid b$. Agora se $c \in \mathbb{Z}$ tal que $c \mid a$ e $c \mid b$, então $a = c\lambda_1$ e $b = c\lambda_2$, onde $\lambda_1\,, \lambda_2 \in \mathbb{Z}$. Assim,

$$\begin{aligned} d \;&=\; ax_o + by_o \\ &=\; c\lambda_1\, x_o + c\lambda_2 y_o \\ &=\; c\,(\lambda_1\, x_o + \lambda_2 y_o)\,, \end{aligned}$$

isto é, $c \mid b$. Portanto $d = mdc\,(a, b)$. □

Da mesma maneira, pode-se definir o máximo divisor comum entre n inteiros. No entanto, isto não será considerado neste texto. Para tanto, indicamos a referência [5].

1.5 Mínimo Múltiplo Comum

O conceito de Mínimo Múltiplo Comum (mmc) é um resultado que decorre de um processo análogo ao conceito de mdc, bastante conhecido no ensino fundamental e médio.Quanto a sua aplicação neste nível de ensino, é normal existirem poucos e simples exemplos de contextualização. Vejamos então:

Sejam a e b dois inteiros não nulos, e tomemos os conjuntos

$$W_a = \{n \in \mathbb{N} : a \mid n\} \quad \text{e} \quad W_b = \{n \in \mathbb{N} : a \mid n\}.$$

Consideremos que $|ab| \in W_a$ e $|ab| \in W_b$, afim de que $|ab| \in W_a \cap W_b \subset \mathbb{N}$. Daí, pelo PBO, o conjunto $M_a \cap M_b$ possui menor elemento, denominado de *mínimo múltiplo comum (mmc) de* a e b, que será indicado por $mmc\,(a, b)$.

Em suma:

Definição 1.4. *Sejam* $a, b \in \mathbb{Z}$, *com* $a \neq 0$ *e* $b \neq 0$. *O número* m *é o* ***mínimo múltiplo comum*** *de* a *e* b, *quando as seguintes condições são satisfeitas:*

(a) $a \mid m$ e $b \mid m$.

(b) Se $c \in \mathbb{N}$ é um múltiplo comum de a e b tal que $a \mid c$ e $b \mid c$, então $m \mid c$.

Por exemplo,

$$mmc(5, 7) = 35, \quad mmc(8, 16) = 16 \quad \text{e} \quad mmc(8, -16) = 16.$$

Podemos mostrar sem muitas dificuldades que, para quaisquer $a, b \in \mathbb{Z}^*$,

$$mmc(a, b) = mmc(-a, b) = mmc(a, -b) = mmc(-a, -b).$$

Portanto, para o cálculo do mmc, podemos considerar sempre $a > 0$ e $b > 0$.

O Teorema a seguir, mostrar a existência do mínimo múltiplo comum m para quaisquer dois inteiros não nulos a e b, o qual denotamos por $m = mmc\,(a, b)$.

Teorema 1.4. *Sejam* $a, b \in \mathbb{Z}$, *com* $d = mdc(a, b)$. *Então existe* $m = mmc(a, b)$, *temos que*

$$m = \frac{ab}{d}.$$

Demonstração: Notemos que $m_1 = \dfrac{|ab|}{d}$ e provemos que $m_1 = m$. Como $d \mid a$ e $d \mid b$, então $a = d\lambda_1$ e $b = d\lambda_2$, com $\lambda_1, \lambda_2 \in \mathbb{N}$. Assim,

$$m_1 = \frac{ab}{d} = \frac{\lambda_1 db}{d} = \lambda_1 b \Rightarrow b \mid m_1.$$

Além disso,temos,

$$m_1 = \frac{ab}{d} = \frac{a\lambda_2 d}{d} = a\lambda_2 \Longrightarrow a \mid m_1.$$

Tomemos agora m_2 outro múltiplo comum de a e b, isto é, $m_2 = a\alpha_1$ e $m_2 = b\alpha_2$, com $\alpha_1, \alpha_2 \in \mathbb{N}$.

Pela a identidade de Bachet-Bézout, existem inteiros x e y tais que $d = ax + by$. Logo,

$$\begin{aligned} \frac{m_2}{m_1} = \frac{m_2 d}{m_1 d} &= \frac{axm_2 + bym_2}{ab} \\ &= \frac{ab\alpha_2 x + ab\alpha_1 y}{ab} \\ &= \frac{ab\,(\alpha_2 x + \alpha_1 y)}{ab} \\ &= \alpha_2 x + \alpha_1 y, \end{aligned}$$

isto é, $m_1 \mid m_2$. Isso mostra que o mínimo múltiplo comum m entre a e b existe $m = ab/d$. $\triangle$

Conforme o Teorema 1.4 , $mmc\,(a, b) \leqslant ab$. Ora, o cálculo de $d = mdc(a, b)$, o que é executado de modo prático através do algoritmo de Euclides que apresentaremos na Seção 3.2 , acarretando diretamente na resolução de $m = mmc(a, b)$. Portanto, basta dividir o produto ab por d.

Uma consequência direta do teorema anterior é o seguinte resultado:

Corolário 1.2. *Sejam $a, b \in \mathbb{N}$, temos que $mmc\,(a, b) = ab$ se, e somente se, a e b são primos entre si.*

De fato, basta observar que $mdc\,(a, b) = 1$.

Exemplo 1.1. *Calcular o $mmc(426, 146)$.*

Solução: Como $mdc(426, 144) = 3$, então

$$mmc(426, 146) = \frac{426 \cdot 144}{3} = 20448.$$

$\triangle$

De forma similar, podemos definir o mínimo múltiplo comum entre n inteiros, entretanto, isto não será considerado neste texto. Por conseguinte indicamos a referência [5]

Capítulo 2

Números Primos

Nesta seção, vamos destacar os números primos que, conforme o Teorema Fundamental da Aritmética, são os principais números inteiros. É importante ressaltar que a idéia primalidade considerada sobre os números inteiros se estende para ambientes mais amplo, especificamente, para extensões dos números inteiros. Essa ideia pode ser encontrada na referência [5]. Ainda nessas generalizações, o conceito de primalidade tem muitas aplicações nos outros ramos da Teoria dos Números, como por exemplo, na Teoria Algébrica dos Números e na Teoria Analítica dos Números, sendo de grande relevância na matemática, pois, ainda existem alguns resultados desses números que não tem solução. No entanto, para não fugir aos objetivos do nosso trabalho, vamos direcionar nosso estudo nos conceitos e resultados sobre os números primos, os quais daremos destaque ao Teorema Fundamental da Aritmética e o Crivo de Eratóstenes, como um resultado da Divisão Euclidiana.

2.1 Teorema Fundamental da Aritmética

Consideremos o número 28 e observe que ele pode ser fatorado nas seguintes formas:

$$28 = 1 \cdot 28, \quad 28 = 2 \cdot 14, \quad 28 = 7 \cdot 4.$$

Nota-se que, além da fatoração canônica $28 = 1 \cdot 28$, existem as fatorações $28 = 2 \cdot 14$ e $28 = 7 \cdot 4$, isto é, o número 28 possui divisores diferentes de 1 e dele próprio, enquanto com o número 13, por exemplo, $13 = 1 \cdot 13$, isto já não acontece, pois os seus únicos divisores são 1 e ele mesmo. Isto motiva a seguinte definição:

Definição 2.1. *Um número $p \in \mathbb{Z} - \{0, \pm 1\}$ é chamado* ***primo*** *quando seus únicos divisores positivos são* 1 *e* $|p|$*. Caso contrario, dizemos que* p *é* ***composto.***

Observemos que o número 1 não é primo nem composto (de acordo com existência elemento neutro da multiplicação), e que 2 e -2 são os únicos primos pares. Além disso, $a \in \mathbb{Z}$ é composto se, e somente se,

$$a = bc \quad com \quad b, c \in \mathbb{Z} \quad e \quad 1 < |b|, |c| < |a|.$$

Os números primos serão indicados sempre pelas letras p e q , a não ser que mencionamos o contrário.

Exemplo 2.1. *Os números 7,-11 e 5 são primos, já* $14 = 7 \cdot 2, 4 = 2 \cdot 2, 16 = 4 \cdot 4$ *são compostos.* $\triangle$

Exemplo 2.2. *Note que o número* $a = 36^8 - 25^2$ *é composto. Pois, escrevendo a como uma diferença de quadrados, temos*

$$a = \left(6^8\right)^2 - 25^2 = \left(6^8 + 25\right)\left(6^8 - 25\right).$$

Portanto, $b = (6^8 + 25)$ *é uma divisor próprio de a.* $\triangle$

Exemplo 2.3. *Mostre que se* $m - 1$ *e* $m + 1$ *são primos, com* $m > 4$*, então* m *é multiplo de* 6*.*

Solução: Por Algoritmo da Divisão, temos que $m = 6q + r, \quad com \quad r \in \{0, 1, 2, 3, 4, 5\}$. Logo,

$$m - 1 = 6q + r - 1 \quad e \quad m + 1 = 6q + r + 1.$$

Desde que $m - 1 > 3$ e $m + 1 > 5$ são ambos primos, então r só pode assumir o valor $r = 0$,isto é, $m = 6q$. $\triangle$

Já que p é primo se, e somente se, $-p$ é primo, consideremos apenas os números primos positivos, e seu conjunto destes terá a seguinte notação P. **Posteriormente, mostraremos que o conjunto P é infinito.** Os onze primeiros números primos são:

$$P = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 31, 37 \ldots\}.$$

Notemos que o conjunto dos números compostos também é infinito, porque cada inteiro da maneira $2k$ (um inteiro par), para $k > 1$, tem o número 2 como um divisor próprio.

Se a é um número composto e a divide o produto bc, então não necessariamente $a \mid b$ ou $a \mid c$. Por exemplo, $9 \mid 6 \cdot 3$, mas $9 \nmid 6$ e $9 \nmid 3$. Vamos observar um caso particular. O primo $p = 5$ divide 200, na qual pode ser escrito como as multiplicações seguintes:

$$200 = 2 \cdot 100 = 4 \cdot 50 = 5 \cdot 40 = 8 \cdot 25$$

A cada uma dessas multiplicações, temos $p = 5$ dividindo ao menos um dos fatores. Formalizando, obtemos a seguinte proposição:

Proposição 2.1. *Sejam $a_1, a_2 \in \mathbb{Z}$ e p um número primo. Se $p \mid a_1a_2$, então $p \mid a_1$ ou $p \mid a_2$.*

Demonstração: Como p é primo, $mdc\,(a_1, p) = 1$ ou $mdc\,(a_1, p) = p$. Se $p \nmid a_1$ então $mdc\,(a_1, p) = 1$. Como $a, b \in \mathbb{Z}$, são ditos **primos entre si** ou **relativamente primos** quando $mdc\,(a, b) = 1$. Logo, temos que $p \mid a_2$. □

Generalizando o resultado anterior para um produto de n inteiros, temos

Corolário 2.1. *Se p é primo um tal que $p \mid a_1a_2a_3 \ldots a_n$, então existe um índice k com $1 \leqslant k \leqslant n$, tal que $p \mid a_k$.*

A demonstração pode ser encontrada em [1].

Corolário 2.2. *Se $p, q_1, q_2, q_3, ..., q_r$ são números primos e $p \mid q_1q_2q_3...q_r$, então $p = q_k$ para algum $k, 1 \leqslant k \leqslant n$.*

Demonstração: De fato, pelo Corolário 2.1, existe um índice k, com $1 \leqslant k \leqslant r$, tal que $p \mid q_k$, como os únicos divisores positivos de q_k são 1 e q_k. Daí, segue que $p = 1$ ou $p = q_k$. Mas, $p > 1$, pois p é primo. Logo, $p = q_k$. □

O resultado da Proposição 2.1 é parte da determinação dos números primos a partir do teorema seguinte.

Teorema 2.1. *Um inteiro $p > 1$ é primo se, e somente se, toda vez que p dividir um produto de dois números, dividirá ao menos um deles.*

Demonstração: Sabendo que se p é primo e divide o produto de dois inteiros, então p divide ao menos um deles. Reciprocamente, consideremos que dados inteiros a e b, com $p \mid ab$, então $p \mid a$ ou $p \mid b$. Suponhamos, por absurdo, que p não é primo. Logo, podemos escrevê-lo na forma

$$p = cd \quad \text{com} \quad 1 < c, d < p.$$

Assim, $p \mid cd$, mas $p \nmid c$ e $p \nmid d$, o que é contradição. □

Teorema 2.2. *Se $a > 1$,então existe um primo p tal que $p \mid a$.*

A demonstração pode ser encontrada em [3]

Teorema 2.3 (Fundamental da Aritmética - TFA)**.** *Todo número natural maior do que 1 pode ser escrito de forma única, a menos da ordem dos fatores, como um produto de números primos. Especificamente,*

$$a = p_1 p_2 ... p_n,$$

em que $p_1, p_2, ..., p_n$ são primos.

A demonstração pode ser encontrada em [5].

O TFA nos garante que, se a é um número primo, então o produto de números primos, resulta o próprio a .

Os primos que surgem na decomposição canônica de um dado inteiro $a > 1$, nem sempre, são distintos. Por exemplo, $400 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 = 2^4 \cdot 5^2$. Portanto, organizando os primos, cujo à repetição na fatoração de a. Podemos, assim enunciar o Teorema 2.3 da seguinte maneira:

Corolário 2.3. *Todo número natural, $a > 1$ pode ser escrito de modo único, a menos da ordem dos fatores, na seguinte maneira*

$$a = p_1^{r_1} p_2^{r_2} ... p_k^{r_k}, \tag{2.1}$$

em que $p_1, p_2, ..., p_k$ são primos distintos e $r_1, r_2, ..., r_k$ são números naturais.

A representação de um inteiro $a > 1$ dada em 2.1 é denonimada à sua **fatoração** ou **decomposição canônica** em fatores primos.

Exemplo 2.4. *Mostre que $\sqrt{3}$ é irracional.*

Solução: Se $\sqrt{3} = a/b$, com $mdc\,(a, b) = 1$, então $3 \cdot b^2 = a^2$, isso mostra que 3 divide a^2. Sendo 3 primo, então 3 divide a^2, isto é, $a = 3k$. Substituindo este valor em $3 \cdot b^2 = a^2$, obtemos que $b^2 = 3k^2$, ou seja, 3 também divide b. Logo, $mdc\,(a, b) \neq 1$, o que é uma contradição. $\triangle$

Teorema 2.4. *Se $a = p_1^{r_1} p_2^{r_2} ... p_n^{r_n}$ é a fatoração canônica de $a > 1$, então um inteiro d é um divisor positivo de a se, e somente se,*

$$d = p_1^{s_1} p_2^{s_2} \dots p_n^{s_n},$$

em que $0 \leqslant s_i \leqslant r_i$ para cada $i = 1, \dots, n$.

Demonstração: Se $d = p_1^{s_1} p_2^{s_2} \dots p_n^{s_n}$, com $0 \leqslant s_i \leqslant r_i$, então $r_i = s_i + k_i$ para cada $i = 1, 2, \dots, n$. Dessa maneira,

$$\begin{aligned} a &= p_1^{r_1} p_2^{r_2} \dots p_n^{r_n} = p_1^{(s_1+k_1)} p_2^{(s_2+k_2)} \dots p_n^{(s_n+k_n)} \\ &= \left(p_1^{s_1} p_2^{s_2} \dots p_n^{s_n}\right) \left(p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}\right) \\ &= d \cdot p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}, \end{aligned}$$

ou seja, $d \mid a$.

Reciprocamente, vamos supor que $d \mid a$, isto é, $a = dc$ para algum c.

Conforme o TFA, obtemos

$$c = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n} \quad e \quad d = p_1^{s_1} p_2^{s_2} \dots p_n^{s_n},$$

no qual $0 \leqslant s_i$ e $0 \leqslant k_i$para cada $i = 1, 2, ..., n$. Logo,

$$p_1^{r_1} p_2^{r_2} ... p_n^{r_n} = \left(p_1^{s_1} p_2^{s_2} \dots p_n^{s_n}\right) \left(p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}\right) = p_1^{(s_1+k_1)} p_2^{(s_2+k_2)} \dots p_n^{(s_n+k_n)}.$$

Pelo TFA, devemos necessariamente ter

$$r_i = s_i + k_i \text{ para cada } i = 1, 2, \dots, n.$$

$$\text{Como } 0 \leqslant k_i, \text{ então } s_i \leqslant r_i \text{ para cada } i = 1, \dots, n. \qquad \square$$

Exemplo 2.5. *Em conformidade com o Teorema 2.4, os divisores positivos de* $a = 80 = 2^4 \cdot 5$ *são:*

$$\begin{aligned} d_1 &= 2^0 \cdot 5^0 = 1, & d_2 &= 2^1 \cdot 5^0 = 2, \\ d_3 &= 2^2 \cdot 5^0 = 4, & d_4 &= 2^3 \cdot 5^0 = 8, \\ d_5 &= 2^4 \cdot 5^0 = 16, & d_6 &= 2^0 \cdot 5^1 = 5, \\ d_7 &= 2^1 \cdot 5^1 = 10, & d_8 &= 2^2 \cdot 5^1 = 20, \\ d_9 &= 2^3 \cdot 5^1 = 40 & d_{10} &= 2^4 \cdot 5^1 = 80. \end{aligned}$$

$\triangle$

Por vezes, se um determinado primo p_k não ocorre na fatoração de $a \in \mathbb{N}$ com expoente maior que 0, é adequado escrever na seguinte maneira

$$a = p_1^{r_1} p_2^{r_2} ... p_n^{r_n} p_k^0.$$

Assim, dados $a, b \in \mathbb{N}$, com $a > 1$ e $b > 1$, sempre é possível escrevê-los como

$$a = p_1^{r_1} p_2^{r_2} ... p_n^{r_n} \quad e \quad b = p_1^{s_1} p_2^{s_2} ... p_n^{s_n},$$

sendo $p_1, p_2, ..., p_n$ primos distintos e $r_i, s_i \in \mathbb{N} \cup \{0\}$.

Por exemplo, $a = 312 = 2^2 \cdot 7 \cdot 11 \quad e \quad b = 176 = 2^4 \cdot 11$, temos

$$a = 312 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7 \cdot 11 \quad e \quad b = 176 = 2^4 \cdot 3^0 \cdot 5^0 \cdot 7^0 \cdot 11.$$

Para o resultado seguinte, estas considerações nos são necessárias.

Teorema 2.5. *Sejam* $a = p_1^{r_1} p_2^{r_2} ... p_n^{r_n} \quad e \quad b = p_1^{s_1} p_2^{s_2} \dots p_n^{s_n}$, *sendo* $p_1, p_2, \dots, p_n$ *primos distintos e* $r_i, s_i \in \mathbb{N} \cup \{0\}$.*Então,*

$$mdc\,(a,b) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}, \quad com \quad \alpha_i = \min\{r_i, s_i\}, \quad 1 \leqslant i \leqslant n,$$

e

$$mmc\,(a,b) = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}, \quad com \quad \beta_i = \max\{r_i, s_i\}, \quad 1 \leqslant i \leqslant n,$$

onde, $\min\{r_i, s_i\}$ *e* $\max\{r_i, s_i\}$ *indicam o mínimo e o máximo entre* r_i *e* s_i, *respectivamente.*

A demonstração podemos encontrar em [5].

Para calcular o mdc e o mmc entre dois inteiros utilizando o Teorema 2.5, é preciso determinar a fatoração canônica de cada um deles. A complexidade deles, provém exatamente disto, pois fatorar algum número como produto de potências de primos, em geral, é difícil. Percebendo assim que o Algoritmo de Euclides é a maneira mais eficaz, que será e demonstrado na Seção 3.2.

Capítulo 3

Divisão Euclidiana: Algumas Aplicações

3.1 Sistema de Numeração

Alguns resultados aritméticos elementares foram determinados pelos antigos gregos, com a representando dos números foi estabelecido um método de facilitar as operações aritméticas entre eles, ou seja, soma, subtração, multiplicação e divisão. Nesta linha de raciocínio, o sistema de numeração decimal é com certeza o mais eficaz.

O sistema de núméração decimal é constituido por dez algarismos que podem ser ordenados de maneiras distintas, formados números de qualquer classe e ordem. A saber são esses:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9.$$

Quando um número natural é composto por eles, afirmamos que é escrito na representação decimal. Por exemplo, $a = 47372$ está na representação decimal, podendo ainda ser colocado na base 10, obtendo assim:

$$a = 4 \cdot 10^4 + 7 \cdot 10^3 + 3 \cdot 10^2 + 7 \cdot 10 + 2.$$

Generalizando, um número natural $a = r_n r_{n-1} ... r_1 r_0$ no sistema decimal é formado unicamente como um somatório finito, em que cada parcela é múltiplo da potência de 10, mais propriamente,

$$a = r_n 10^n + r_{n-1} 10^{n-1} + \cdots + r_1 10 + r_0,$$

com os r_i's (os algarismos de a) são inteiros com $0 \leqslant r_i \leqslant 9$, para $i = 1, ..., n$.

O teorema seguinte é uma aplicação deste trabalho e a demonstração encontra-se em [5]. Podemos representar os números naturais de diversas maneiras. Cada uma delas é chamada de *sistema de numeração.* Alías, pode-se provar que estas, existem em comum o caso de os números naturais serem denotado por números (Digítos ou Algarismos) que pertecem ao conjunto finito de inteiros.

Teorema 3.1. *Seja b um inteiro, com $b > 1$. Então todo inteiro positivo a pode ser escrito de modo na forma*

$$a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b_0 + r_0,$$

em que $n \geqslant 0$, $r_n \neq 0$ e para cada i, com $0 \leqslant i \leqslant n$, temos que $0 \leqslant r_i < b$ e $n = [\log_b a]$.

Nas condições do Teorema 3.1, a expressão

$$a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b_0 + r_0,$$

é chamada **expansão de** a na base b ou expansão b**-ádica** de a, a qual indicaremos por

$$(r_n r_{n-1} ... r_1 r_0)_b,$$

em que $n + 1$ é o número de dígitos, sendo $r_n > 0$ o primeiro dígito, r_{n-1} o segundo, e assim sucessivamente. Desde que $b = 1 \cdot b + 0$, então $b = (10)_b$.

Observemos que, a demonstração do Teorema 3.1, nos traz a vantagem de ser algorítmica no sentido de dar um metodologia para calcular a expansão $b-$ádica de a.

Quando não indicarmos a base b, então ela é a usual, isto é, a decimal $b = 10$, de modo que $(r_n r_{n-1} ... r_1 r_0)_{10}$, assim, podendo ser escrito da seguinte forma $r_n r_{n-1} ... r_1 r_0$. Ora, se $b > 10$, então indicaremos $a = (r_n r_{n-1} ... r_1 r_0)_b$ é útil representar os algarismos $r_i > 9$ por letras, especificamente, x, y, w, z, etc, para não gerar dúvida. Por exemplo, se $b = 12$, então, dado que,

$$49978 = 2 \cdot 12^4 + 4 \cdot 12^3 + 11 \cdot 12^2 + 0 \cdot 12 + 10,$$

escrevemos $49978 = (24x0y)_{12}$, com $x = 11$ e $y = 10$.

Existem algumas bases que têm nomes especiais, tais como a decimal, a binária com $b = 2$, ternária se $b = 3$, octal se $b = 8$ e a hexadecimal sendo $b = 16$.

O sistema binário, é um dos mais utilizados, principalmente na aréa da Informatica, pois é a linguagem dos computadores. Para este, cada inteiro positivo a é representado como uma

soma de potências de 2, isto é,

$$a = 2^n + r_{n-1}2^{n-1} + \cdots + r_0,$$

na qual r_i é 1 ou 0 para $i = 0, ..., n-1$.

Exemplo 3.1. *Vamos calcular a expansão 8-ádica do inteiro* $a = 1034$. *Escrever também* $(15263)_7$ *na base 10.*

Solução: Dados $n = [\log_8 1034] = 3$, logo o número de digitos de a na base $b = 8$ é $3 + 1 = 4$. Assim, nas divisões sucessivas, tambem terá o quociente q_3 é igual a zero. Temos,

$$\begin{aligned} 1034 &= 8 \cdot 129 + 2 \qquad (q_0 = 129 \quad \text{e} \quad r_0 = 2), \\ 129 &= 8 \cdot 16 + 1 \qquad (q_1 = 16 \quad \text{e} \quad r_1 = 1), \\ 16 &= 8 \cdot 2 + 0 \qquad (q_2 = 2 \quad \text{e} \quad r_2 = 0), \\ 2 &= 8 \cdot 0 + 2 \qquad (q_3 = 0 \quad \text{e} \quad r_3 = q_2 = 2). \end{aligned}$$

Dessa forma,

$$1034 = 2 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8 + 2,$$

isto é, $1034 = (2012)_8$. Agora,

$$(15263)_7 = 1 \cdot 7^4 + 5 \cdot 7^3 + 2 \cdot 7^2 + 6 \cdot 7 + 3 = 4259.$$

△

3.1.1 Alguns Critérios de Divisibilidade

Nesta seção, consideremos alguns critérios de divisibilidade, baseando-se na representação decimal de um dado número natural e o item (3) do Teorema 1.1 com sua generalização. Conforme o Teorema 3.1, todo número natural a pode ser escrito de maneira única da seguinte forma:

$$a = r_n 10^n + r_{n-1}10^{n-1} + \cdots + r_1 10 + r_0, \tag{3.1}$$

no entanto, $n \geqslant 0$, $r_n \neq 0$, e para cada i, com $0 \leqslant i \leqslant n$, $0 \leqslant r_i < 10$.

Divisibilidade por 2, 5 e 10

Os critérios por 2, 5 e 10 são obtidos diretamente. De fato,

$$r_n 10^n + r_{n-1}10^{n-1} + \cdots + r_1 10,$$

é uma soma na qual todas as parcelas são múltiplos de 2, 5 e 10, respectivamente, resultando de 3.1, temos

$$2 \mid a \Leftrightarrow 2 \mid r_0 \Leftrightarrow r_0 \text{ é par},$$

isto é, 2 divide a se, somente se, $r_0 = 0, 2, 4, 6$ ou 8. Dessa forma,

> *Um inteiro é divisivel por* 2 *se, somente se, seu último algarismo (das unidades) for par.*

Por exemplo, $a = 64234$ é divisivel por 2, já $b = 462137$ o que não é valido para este caso. Da mesma maneira,

$$5 \mid a \Leftrightarrow 5 \mid r_0 \Leftrightarrow r_0 = 0 \text{ ou } r_0 = 5.$$

daí,

> *Um inteiro é divisivel por* 5 *se, somente se, seu último algarismo (das unidades) for* 0 *ou* 5.

Desse modo, $a = 73980$ e $b = 34695$ são divisíveis por 5. Agora, $c = 5426$ e $d = 85738$, o que não é válido para este caso. Por fim,

$$10 \mid a \Leftrightarrow 10 \mid r_0 \Leftrightarrow r_0 = 0,$$

já que $r_0 = 0$ é o único múltiplo de 10. Portanto,

> *Um inteiro é divisivel por* 10 *se, somente se, seu último algarismo (das unidades) for* 0.

Tais como, $a = 20150$ e $b = 74630$ são divisíveis por 10. No entanto, $c = 30985$ e $d = 76592$ estes já não são divisíveis.

Divisibilidade por 3 e 9

Os critérios por 3 e 9 são semelhantes. Primeiro, começaremos mostrando que

$$3 \mid 10^n - 1, \quad \forall\ n \geqslant 0. \tag{3.2}$$

Já que $3 \mid 10^0 - 1 = 0$, então o resultado é valido para $n = 0$. Vamos supor $10^n - 1 = 3k$, isto é, $10^n = 3k + 1$, daí

$$\begin{aligned} 10^{n+1} - 1 = 10^n \cdot 10 - 1 &= (3k+1) \cdot 10 - 1 \\ &= 30k + 3 \\ &= 3\,(10k + 1)\,, \end{aligned}$$

ou seja, $3 \mid 10^{n+1} - 1$. Conclui-se, $3 \mid 10^n - 1$ para todo $n \geqslant 0$.

Consideremos, $a = r_n 10^n + r_{n-1} 10^{n-1} + \cdots + r_1 10 + r_0$, segue que

$$a - (r_n + r_{n-1} + \cdots + r_1 + r_0) = r_n\,(10^n - 1) + r_{n-1}\left(10^{n-1} - 1\right) + \cdots + r_1\,(10 - 1)\,.$$

Em conformidade com 3.2, os termos à direita da última igualdade são sempre divisiveis por 3. Então,

$$a - (r_n + r_{n-1} + \cdots + r_1 + r_0) = 3k \quad \text{com} \quad k \in \mathbb{Z}.$$

Daí, segue que, se 3 divide a, então 3 divide $r_n + r_{n-1} + \cdots + r_1 + r_0$ (soma dos digitos de a). Reciprocamente, se 3 divide $r_n + r_{n-1} + \cdots + r_1 + r_0$, então 3 divide a. O que resulta,

Um inteiro é divisivel por 3 se, somente se, a soma de seus dígitos é divisível por 3

Como 9 divide 3, então $9 \mid 10^n - 1$, assim o critério por 9 é análogo, isto é,

Um inteiro é divisivel por 9 *se,somente se, a soma de seus dígitos é divisível por* 9.

Por exemplo, $a = 468$ e $b = 41583$ são divisíveis por 3, pois

$$4 + 6 + 8 = 18 = 3 \cdot 6 \quad \text{e} \quad 4 + 1 + 5 + 8 + 3 = 21 = 3 \cdot 7.$$

mas, os números $c = 683$ e $d = 809120$ não é possível ser divisível por 3, respectivamente, pois $6 + 8 + 3 = 17$ e $8 + 0 + 9 + 1 + 2 + 0 = 20$. Do mesmo modo, $a = 759087$ e $b = 967876983$ são divisiveis por 9, agora, $c = 5964$ e $d = 2643$, não são divisíveis por 9.

Divisibilidade por 4

O número $a = r_n 10^n + r_{n-1} 10^{n-1} + \cdots + r_1 10 + r_0$ pode ser escrito da seguinte maneira:

$$a = 100k + r_1 r_0,$$

pois, $a = r_n 10^n + r_{n-1}10^{n-1} + \cdots + r_2 10^2$ é divisivel por $100 = 4 \cdot 25$. Portanto, para determinar a divisibilidade por 4, analisaremos o número $r_1 r_0$, que é formado pelos algarismos da dezenas e unidades. Em resumo temos,

> *Um inteiro é divisível por* 4 *se, e somente se, o número formado pelos Algarismos das dezenas e das unidades é divisivel por* 4.

Como 36 é múltiplo de 4, logo $a = 42736$ é divisível por 4. No entanto, $b = 732839$ não é divisível por 4, pois 39 não é múltiplo de 4.

Divisibilidade por 7

Para o resultado do critério por 7, detalharemos um pouco mais. Assim, temos

$$a = r_n 10^n + r_{n-1}10^{n-1} + \cdots + r_1 10 + r_0,$$

ou melhor,

$$a = 10k + r_0,$$

pois, $r_n 10^n + r_{n-1}10^{n-1} + \cdots + r_1 10$ é multiplo de 10, e $k = r_n r_{n-1} \ldots r_2 r_1$ (o número formado pelos algarismo de a, exceto o das unidades). Mostraremos que

$$7 \mid a \Leftrightarrow 7 \mid k - 2r_0.$$

Com efeito, se 7 divide a, então existe um inteiro m tal que $a = 7m$. Daí, como $r_0 = a - 10k$,

$$\begin{aligned} k - 2r_0 &= k - 2(a - 10k) &&= k - 2(7m - 10k) \\ &&&= 21k - 14m \\ &&&= 7(3k - 2m), \end{aligned}$$

ou seja, 7 divide $k - 2r_0$. Por outro lado, se $7 \mid k - 2r_0$, então $k - 2r_0 = 7\alpha$, com $\alpha \in \mathbb{Z}$, isto é, $k = 7\alpha + 2r_0$. Dessa maneira,

$$a = 10k + r_0 = 10(7\alpha + 2r_0) + r_0 = 7(10\alpha + 3r_0).$$

Logo, concluí-se que 7 divide a.

O processo apresentado anteriormente devemos repetir, até que o número seja fácil identificar a divisibilidade por 7, algumas vezes, respectivamente.

Por exemplo, $a = 16079$ é divisível por 7. Diante disso, temos que $k = 1607$ e $r_0 = 9$. Logo,

$$k - 2r_0 = 1607 - 2 \cdot 9 = 1589,$$

visto que, o número 1589 é menor que 16079, mas ainda é dificil identificar a divisibilidade por 7. Portanto, aplicaremos novamente o processo. Note que, $k = 158$ e $r_0 = 9$, assim

$$k - 2r_0 = 158 - 2 \cdot 9 = 140,$$

repetindo o processo com $k = 14$ e $\mathrm{r}_0 = 0$, temos

$$k - 2r_0 = 14 - 2 \cdot 0 = 14$$

Logo, $7 \mid 14$, daí,$7 \mid 140$, acarretando que $7 \mid 1589$, por fim, $7 \mid 16079$. Agora, para $a = 12643$, aplicando de maneira sucessiva, obtemos

$$\begin{aligned} 1264 &- 2 \cdot 3 = 1258, \\ 125 &- 2 \cdot 8 = 109, \\ 10 &- 2 \cdot 9 = -8. \end{aligned}$$

Pois $7 \nmid -8$, podemos concluir que $7 \nmid 12643$.

3.2 Algoritmo de Euclides

Existe alguns dados históricos referente ao conhecimento sobre a vida do matemático Euclides de Alexandria (fl. c. 300 AC), mas é imensamente vasta as consequências advindas de seus estudos. Dentre suas obras, destaca-se *Os Elementos*, livro que fundamentou toda a Geometria Euclidiana Plana que conhecemos hoje em dia. Esse livro se compõe de 13 capítulos, no qual o sétimo apresenta o processo conhecido como *Algoritmo Euclidiano*, processo fundamental para encontrarmos o máximo divisor comum de número inteiros, podendo ser usado para verificarmos se dois números são primos entre si. Diante disso, iniciaremos um estudo em tal algoritmo, sendo uma das principais aplicações da divisibilidade euclidiana.

Para determinar $d = mdc\,(a, b)$, quando $a > 0$ e $b > 0$ são relativamente "pequenos" a resolução é feita sem muitas complicações. Agora para encontrar d quando temos $a = 4838$ e $b = 308572$, onde a e b são consideràvelmente grandes torna-se bastante impraticável e tedioso.

A seguir mostraremos um resultado bastante notável, sendo fundamentado para atingir de uma forma mais satisfatória para calcular $d = mdc\,(a, b)$, para quaisquer que sejam os inteiros a e b, que baseia-se em divisões sucessivas.

Lema 3.1 (Euclides)**.** *Se* $a = bq + r$, *então* $mdc(a, b) = mdc(b, r)$.

Demonstração: Por 1.4, todo divisor de b e r é também divisor de a. Por outro lado, se $d \in \mathbb{N}$ é tal que $d \mid a$ e $d \mid b$, então, como $r = a - bq$, segue que $d \mid r$. Isto é suficiente para que tenha $mdc\,(a, b) = mdc\,(b, r)$. □

Podemos concluir pelo Lema 3.1 que o problema em determinar $mdc\,(a, b)$ reduz a calcular $mdc\,(b, r)$.

Consideremos $a, b \in \mathbb{Z}$, com $a > b > 0$. Pela divisão euclidiana, obtemos

$$a = b \cdot q_0 + r_0, \quad \text{com} \quad a \leqslant r_o < b.$$

Conforme o Lema 3.1, $mdc\,(a, b) = mdc\,(b, r_0)$. Desse modo, vamos considerar dois casos:

1. Se $r_0 = 0$, então
$$mdc\,(a, b) = mdc\,(b, r_0) = mdc\,(b, 0) = b.$$

2. Se $r_0 \neq 0$, dessa maneira vamos efetuar a divisão de b por r_0, daí
$$b = r_0 \cdot q_1 + r_1, \quad \text{com} \quad 0 < r_1 \leqslant r_0.$$

Assim,

3. Se $r_0 \neq 0$ segue-se que
$$mdc\,(a, b) = mdc\,(b, r_0) = mdc\,(r_0, r_1) = mdc\,(r_0, 0) = r_0.$$

4. Se $r_1 \neq 0$, efetuamos a divisão de r_0 por r, temos
$$r_0 = r_1 \cdot q_2 + r_2 \quad \text{com} \quad 0 \leqslant r_2 < r_1,$$

procedemos, mais uma vez conforme fizemos anteriormente, temos

$$mdc\,(a, b) = mdc\,(b, r_0) = mdc\,(r_0, r_1) = mdc\,(r_1, r_2)\,,$$

e assim sucessivamente. Desse modo, existe um índice n tal que $r_n \neq 0$ e $r_{n+1} = 0$, o que não é possível.

Por conseguinte temos:

$$mdc\,(a,b) = mdc\,(b,r_0) = mdc\,(r_0,r_1) = mdc\,(r_1,r_2) = \cdots = mdc\,(r_n,r_{n+1}) = mdc\,(r_n,0) = r_n$$

Conclui-se que o último resto não é nulo r_n é o mdc de a e b. Em resumo, temos o resultado seguinte, cuja demonstração pode ser encontrada em [4]

Teorema 3.2 (Algoritmo de Euclides)**.** *Sejam $r_0 = a$ e $r_1 = b$ inteiros não negativos, com $b \neq 0$. Se o algoritmo da divisão for aplicado sucessivamente para obter-se,*

$$r_j = q_{j+1}r_{j+1} + r_{j+2}, \qquad 0 \leqslant r_{j+2} < r_{j+1},$$

para $j = 0, 1, 2, ..., n-1$ e $r_{n+1} = 0$ então $(a,b) = r_n$, o último resto não-nulo.

A seguir, vamos exemplificar com o cálculo de mdc por intermédio do algoritmo de Euclides.

Exemplo 3.2. *Calcular $d = mdc(1036, 246)$ e expressá-lo conforme o Teorema 1.3.*

Solução: Note que $1036 > 246$, usando o Algoritmo de Euclides, dividindo $a = 1036$ por $b = 246$. Segue-se que:

$$\begin{aligned}
1036 &= 246 \cdot 2 + 52 \implies mdc\,(1036,246) = mdc\,(246,52)\,,\\
246 &= 52 \cdot 4 + 36 \implies mdc\,(246,52) = mdc\,(52,36)\,,\\
52 &= 36 \cdot 1 + 12 \implies mdc\,(52,36) = mdc\,(36,12)\,,\\
36 &= 12 \cdot 3 + 0 \implies mdc\,(136,12) = mdc\,(12,0) = 12,
\end{aligned} \tag{3.3}$$

Logo, $mdc(1036, 246) = 12$.

Agora vamos encontrar x_o e $yo \in \mathbb{Z}$ tais que $12 = 1036 \cdot x_o + 246 \cdot y_o$. Isso, consiste em isolar os restos não nulos da divisão de baixo para cima das igualdades em 3.3, substituindo-os

sucessivamente. Temos,

$$\begin{aligned} 12 &= 52 - 36 \cdot 1 &&= 52 - 36 \cdot (246 - 4 \cdot 52) \\ &&&= 52 - 36 \cdot 246 - 36\,(-52 \cdot 4) \\ &&&= 145 \cdot 52 - 36 \cdot 246 \\ &&&= 145 \cdot 52 - (1 \cdot 246 - 4 \cdot 52) \cdot 246. \\ &&&= 145 \cdot 52 - 246 \cdot 1 \cdot 246 + 984 \cdot 52 \\ &&&= 1129 \cdot 52 - 246 \cdot 246 \\ &&&= 1129\,(1036 - 246 \cdot 4) - 246 \cdot 246 \\ &&&= 1129 \cdot 1036 - 4762 \cdot 246, \end{aligned}$$

Daí, podemos afirmar que,

$$12 = 1129 \cdot 1036 - 4762 \cdot 246.$$

Por conseguinte, temos que $x_0 = 1129$ e $y_0 = 4732$. △

Definição 3.1. *Dois inteiros a e b são ditos primos entre si ou relativamente primos quando $mdc\,(a, b) = 1$.*

Por exemplo, 10 e 3 são primos entre si, pois $mdc\,(10, 3) = 1$; Note que, para os números 20 e 3 não são primos entre si, já que $mdc\,(20, 3) = 2$.

Como consequências imediatas do Teorema 1.3 temos:

Corolário 3.1. *Os inteiros a e b são relativamente primos se, e somente se, existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$.*

A demonstração podemos encontrar em [5]

Corolário 3.2. *Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid bc$ e $mdc(a, b) = 1$, então $a \mid c$.*

Demonstração: Por hipótese, $bc = ak$, com $k \in \mathbb{Z}$. Alías, pelo o corolário 3.1, existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Daí, multiplicando ambos os membros desta igualdade por c, temos

$$\begin{aligned} c &= cax + cby &&= cax + aky \\ &&&= a\,(cx + ky)\,. \end{aligned}$$

Logo, $a \mid c$. □

Corolário 3.3. *Sejam $a, b \in \mathbb{Z}$ tais que $mdc\,(a, b) = 1$. Se $a \mid c$ e $b \mid c$ então $ab \mid c$.*

Demonstração: Como $mdc\,(a,b) = 1$, então pela a identidade de Bachet-Bézout, existem $x, y \in \mathbb{Z}$ tais que

$$1 = ax + by, \tag{3.4}$$

por outro lado, λ_1 e $\lambda_2 \in \mathbb{Z}$ tais que $c = a\lambda_1 = b\lambda_2$, dessa maneira

$$cb = ab\lambda_1 \text{ e } ca = ab\lambda_2,$$

multiplicando ambos os membros da igualdade em 3.4 por c, temos que

$$\begin{aligned} c &= cax + cby &= ab\lambda_2 x + ab\lambda_1 y \\ &&= ab\left(\lambda_2 x + \lambda_1 y\right). \end{aligned}$$

Portanto, $ab \mid c$. □

3.3 Crivo de Erastótenes

É normal dentro da Teoria dos Números, nos questionar se algum número natural é primo ou não. Vamos analisar através do Crivo de Erastótenes, que foi um matématico, astrônomo, historiador, geógrafo e filósofo grego, que contribui para a Teoria Elementar dos Números com a determinação dos números primos menores ou iguais a qualquer número natural n. Ressaltemos um resultado importante que é o Teste de Primalidade, segue-se:

Teorema 3.3 (Teste de Primalidade)**.** *Se $n > 1$ for composto, então n possui, necessariamente, um divisor primo p tal que $p \leqslant \sqrt{n}$. Isto é, se n não possui divisores diferentes de 1, menores ou iguais a $\sqrt{n}$, então n é primo.*

Demonstração: Como n é um número composto, então

$$n = a \cdot b, \quad \text{com} \quad 1 < a, b < n.$$

Se $a > \sqrt{n}$ e $b > \sqrt{n}$, então

$$n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n,$$

o que é impossível. Portanto, $a \leqslant \sqrt{n}$ou $b \leqslant \sqrt{n}$. Vamos supor que $a \leqslant \sqrt{n}$. Como $a > 1$, existe pelo Teorema 2.2 um primo p, com $p \mid a$. Desde que $a \mid n$, temos que $p \mid n$ e $p \leqslant a \leqslant \sqrt{n}$.
□

O Teorema 3.3 nos garante que, para provar se algum número $n > 1$ é primo, é bastante notável a sua divisibilidade pelos primos $p \leqslant \sqrt{n}$.

Enquanto n cresce, $\sqrt{n}$ também cresce, mesmo com menor intensidade, isto é,

$$\lim_{x\to\infty} \frac{x}{\sqrt{x}} = \infty.$$

Portanto, o Teste de Primalidade dado pelo teorema anterior perde a eficiência, quando os números de n aumentam consideravelmente. Por exemplo, para $n = 40963956$, temos $[\sqrt{n}] = 6400$, dessa forma, determinamos todos os primos menores ou iguais a 6400 é algo inviável na prática (sem o auxílio do computador, é obvio). Como já falamos, ainda não existe um algoritmo sobre primalidade que seja eficiente do ponto de vista computacional. Por exemplo, o RSA.

Exemplo 3.3. *Para o número $n = 211$, temos que $[\sqrt{n}] = 14$ e os primos menores que 14 são $2, 3, 5, 7, 11$ e 13. Note que estes primos não divide n. Logo, n é primo. Agora, $n = 265$, é composto, pois $[\sqrt{n}] = 16$ e 5 divide 265.* △

É importante destacar o seguinte:

Observação 3.1. *Ao iniciar, excluindo os múltiplos de um determinado número primo p de uma lista de k, podemos começar excluindo a partir de p^2. Dai, se m é composto menor que p^2 que não foi excluído por meio de p, então $m = p_1 q$, sendo p_1 é o menor divisor primo de m. Dessa maneira, pelo Teorema 3.3, $p_1 < \sqrt{m} < p$, ou seja, m necessariamente foi excluído por meio de p_1.*

Para o método de Erastótenes, apresentaremos os passos a seguir que são baseados em todos os primos menores do que n .

Passo 1: Consideremos os números de forma ordenada, a partir de 2, ou seja,

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, \ldots, n. \tag{3.5}$$

Passo 2: Se 2 é o primeiro primo que aparece na sequência de 3.5, então podemos excluí dela todos os seus números pares maiores que 2, restando os seguintes números:

$$2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23 \ldots, n. \tag{3.6}$$

Passo 3: Agora, excluindo o segundo número que aparece na sequência 3.5 que é o 3. Sabemos que, este é primo, sendo assim, excluimos de 3.6 todos os seus múltiplos exceto ele mesmo, assim,

temos,

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29, \ldots, n. \tag{3.7}$$

Passo 4: Por fim, notemos que 5 é o primeiro número que não foi excluído em 3.7, também primo. Removendo os múltiplos de 5 maiores que ele, vamos obter a sequência

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 33, 34, \ldots, n.$$

Repetimos o processo até que o primeiro número não excluído da lista seja maior que $\sqrt{n}$, pois de acordo com o Teorema 3.3, todo os números que restaram são os primos menores ou iguais a n.

Listamos a seguir todos os primos menores que 75, os que são primos destacaremos com retângulos.

	$\boxed{2}$	$\boxed{3}$	4	$\boxed{5}$	6	$\boxed{7}$	8	9	10
$\boxed{11}$	12	$\boxed{13}$	14	15	16	$\boxed{17}$	18	$\boxed{19}$	20
21	22	$\boxed{23}$	24	25	26	27	28	$\boxed{29}$	30
$\boxed{31}$	32	33	34	35	36	$\boxed{37}$	38	39	40
$\boxed{41}$	42	$\boxed{43}$	44	45	46	$\boxed{47}$	48	49	50
51	52	$\boxed{53}$	54	55	56	57	58	$\boxed{59}$	60
$\boxed{61}$	62	63	64	65	66	$\boxed{67}$	68	69	70
$\boxed{71}$	72	$\boxed{73}$	74	75					

Como $\sqrt{75} < 11$, então excluímos todos os múltiplos primos até 7, isto é, os múltiplos de $2, 3, 5$ e 7; Assim, como o primeiro não excluido é 11 e $11^2 > \sqrt{75}$, logo não é necessario considerar os múltiplos de 11.

3.3.1 Fatoração Canônica de $n!$

Conforme o TFA, dado $n > 1$ com fatoração canônica

$$n = p_1^{r_1} p_2^{r_2} p_3^{r_3} ... p_k^{r_k}. \tag{3.8}$$

temos que para cada $i = 1, 2, 3, ...k$, o número r_i é o maior expoente de p_i que surge nesta fatoração. Determinamos a fatoração canônica de $n!$, utilizando este fato.

Iniciaremos com a seguinte:

Definição 3.2. *Seja p um número primo. Dado um número natural n, denotemos por $O_p(n)$ o expoente da maior potência de p que divide n.*

Ora, se $O_p(n) = \alpha$, então $p^{\alpha} \mid n$, mas $p^{\alpha+1} \nmid n$.Por exemplo, para qualquer primo p temos

$$O_p(1) = 0, \qquad O_p(p) = 1, \qquad e \qquad O_p(q) = 0$$

para todo $q \neq p$. Além disso,

$$O_2\left(2^2 \cdot 3\right) = 2, \quad O_2\left(2^9 \cdot 3\right) = 3, \quad O_3\left(2 \cdot 3^6\right) = 6, \quad O_3\left(2 \cdot 3^7\right) = 7.$$

De acordo com a definição anterior, vamos reescrever o inteiro n dado em 3.8 da seguinte maneira:

$$n = p_1^{O_{p_1}(n)} p_2^{O_{p_2}(n)} p_3^{O_{p_3}(n)} \ldots p_k^{O_{p_k}(n)}.$$

Teorema 3.4. *Se p é um número primo, então, para qualquer $m, n \in \mathbb{N}$, temos*

$$O_p(m \cdot n) = O_p(m) + O_p(n).$$

Demonstração: Indicaremos $O_p(m) = \alpha$ e $O_p(n) = \beta$, desde que $p^{\alpha} p^{\beta} = p^{\alpha+\beta}$ é a maior potência de p que divide $m \cdot n$. Dessa maneira,

$$O_p(m \cdot n) = \alpha + \beta = O_p(m) + O_p(n).$$

□

Lema 3.2. *Dados a,b e c inteiros, consideremos b e c positivos e a não negativo. Então,*

$$\left[\frac{\left[\frac{a}{b}\right]}{c}\right] = \left[\frac{a}{bc}\right].$$

Demonstração: Consideremos

$$q_1 = \left[\frac{a}{b}\right] \quad \text{e} \quad q_2 = \left[\frac{\left[\frac{a}{b}\right]}{c}\right].$$

Assim,

$$a = bq_1 + r_1, \qquad com \qquad 0 \leqslant r_1 < b, \tag{3.9}$$

e

$$q_1 = \left[\frac{a}{b}\right] = cq_2 + r_2 \qquad com \qquad 0 \leqslant r_2 < c. \tag{3.10}$$

Portanto, substituindo 3.10 em 3.9, temos

$$a = b\left(cq_2 + r_2\right) + r_1 = bcq_2 + \left(br_2 + r_1\right).$$

Queremos mostrar ainda que $br_2 + r_1 \leqslant bc - 1$. Com efeito, como $0 \leqslant r_1 \leqslant b-1$ e $0 \leqslant r_2 \leqslant c-1m$, daí

$$br_2 + r_1 \leqslant b(c-1) + b - 1 = bc - 1.$$

Assim, concluimos que q_2 é o quociente da divisão de a por bc, ou seja, $q_2 = \left[\frac{a}{bc}\right]$. △

O resultado seguinte é dedicado a Legendre, que foi um matemático francês que contribuiu com resultados importantes para a Teoria dos Números, a Teoria Algébrica e a Teoria Analítica. Este nos mostra como determinar $O_p\left(n!\right)$, ainda que a fatoração canônica de $n!$, não seja dado claramente. e omitiremos a demonstração, que podemos verificar em [2]

Teorema 3.5 (Fórmula de Legendre)**.** *Sejam p primo e $n \geqslant 1$ um número natural. Então*

$$O_p\left(n!\right) = \sum_{k \geqslant 1} \left[\frac{n}{p^k}\right] = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

Em conformidade com a Fórmula de Legendre, calcular $O_p\left(n!\right)$ é algo fácil e, para tanto, consideremos as divisões sucessivas

$$\begin{array}{rcl} n & = & pq_1 + r_1, \quad \text{com} \quad 0 \leqslant r_1 < p, \\ q_1 & = & pq_2 + r_2, \quad \text{com} \quad 0 \leqslant r_2 < p, \\ & \vdots & \\ q_{s-1} & = & pq_s + r_s, \quad \text{com} \quad 0 \leqslant r_s < p, \end{array} \tag{3.11}$$

na qual $q_{s-1} = 0$, pois $q_1 > q_1 > \cdots$, e assim deve existir s tal que $q_s < p$. Substituindo os $q_i's$ em 3.11, temos

$$\begin{array}{rcl} n & = & pq_1 + r_1 \\ & = & p^2q_2 + r_2' \\ & = & p^3q_3 + r_3' \\ & \vdots & \\ & = & p^sq_s + r_s', \end{array}$$

em que $0 \leqslant r_k' < p^k$ para $k = 2, ..., s$, ou seja,

$$O_p\left(n!\right) = q_1 + q_1 + \cdots + q_s.$$

Exemplo 3.4. *Para $n = 15$ e $p = 2$, temos que*

$$O_2(15!) = \left[\frac{15}{2}\right] + \left[\frac{15}{2^2}\right] + \left[\frac{15}{2^3}\right],$$

isto é, $O_2(15!) = 7 + 3 + 1 = 11$. Portanto,

$$15! = 2^{11}k,$$

com $mdc(2, k) = 1$. △

A partir daí, ao dizermos que *"r é o número de zeros de a",* em outras palavras *" a termina com r zeros consecutivos".* Por exemplo, para $a = 120327000$, temos que $r = 3$, e para $a = 53671$, $r = 0$ (a não termina em zero)

Teorema 3.6. *O número de zeros de $n!$ é igual a*

$$\min\{O_2(n!), O_5(n!)\}.$$

Demonstração: Dados $O_2(n!) = \alpha$ e $O_5(n!) = \beta$. O número de zeros de $n!$ é rigorosamente igual a maior potência de $10 = 2 \cdot 5$ que divide $n!$.

Assim, essa potência é igual a

$$10^{\min\{\alpha,\beta\}},$$

logo, o número de zeros de $n!$ é igual a $\min\{O_2(n!), O_5(n!)\}$. □

Como consequência imediata do Teorema 3.6, obtemos o seguinte resultado:

Corolário 3.4. *Se $n \geqslant 5$, então o número de zeros de $n!$ é igual a $O_5(n!)$. Para $n < 5$, $n!$ não tem zero.*

Exemplo 3.5. *Determinar o número de zeros de* 1000!.

Solução: Pelo corolário anterior, o número de zeros de 1000! é igual a $O_5(1000!)$. Assim,

$$O_5(1000!) = \left[\frac{1000}{5}\right] + \left[\frac{1000}{5^2}\right] + \left[\frac{1000}{5^3}\right] + \left[\frac{1000}{5^4}\right] = 200 + 40 + 8 + 1 = 248,$$

logo, o número de zeros de 1000! é 249. △

Exemplo 3.6. *Determinar a fatoração canônica de 20! e verificar com quantos zeros ele termina.*

Solução: Primeiro, vamos determinar $O_p(20!)$, para todo primo $p \leqslant 20$. São eles $p = 2, 3, 5, 7, 11, 13$ e 19. dai,

$$\begin{aligned}
O_2(20!) &= \left[\frac{20}{2}\right] + \left[\frac{20}{2^2}\right] + \left[\frac{20}{2^3}\right] = 10 + 5 + 3 = 18,\\
O_3(20!) &= \left[\frac{20}{3}\right] + \left[\frac{20}{3^2}\right] = 6 + 2 = 8,\\
O_5(20!) &= \left[\frac{20}{5}\right] = 4,\\
O_7(20!) &= \left[\frac{20}{7}\right] = 2,\\
O_{11}(20!) &= \left[\frac{20}{11}\right] = 1,\\
O_{13}(20!) &= \left[\frac{20}{13}\right] = 1,\\
O_{19}(20!) &= \left[\frac{20}{19}\right] = 1.
\end{aligned}$$

Portanto, $20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 19$, e como $O_5(20!) = 4$, temos que $20!$ termina com 4 zeros. △

3.4 Considerações Finais

Esperamos que este trabalho possa atingir os propósitos de fundamentação teórica e principalmente prática, no intuito de suprir as eventuais necessidades de contextualização de conteúdos curriculares nos níveis de ensino, ressaltando a possibilidade de inserir conceitos pertinentes à Teoria dos Números em níveis iniciais com aplicações básicas.

É necessária uma dedicação dos professores em buscar novos caminhos que proporcionem uma aprendizagem significativa. Com isso, a inserção dos conceitos e aplicações tratadas neste, podem auxiliar na busca de resultados mais proveitos no estudo de determinados assuntos.

Referências Bibliográficas

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

[2] FONSECA,R. V. *Teoria dos números.* Editora da Universidade do Pará, Belém, 2011.

[3] MILIES, C. P., COELHO, S. P. *Números: Uma introdução à Matemática.* São Paulo: Editora da Universidade de São Paulo, 2003

[4] SANTOS, J. P. de Oliveira. *Introdução à teoria dos números.* Rio de Janeiro: IMPA, 2007.

[5] VIEIRA, V. L. *Um Curso Básico em Teoria dos Números.* Editora da Universidade Estadual da Paraíba (Co-edição: Livraria de Física da USP), Campina Grande/São Paulo, 2015.