UNIVERSIDADE FEDERAL DE ALAGOAS-UFAL
CAMPUS ARAPIRACA
MATEMÁTICA - LICENCIATURA

JOSÉ ROBÉRIO BEZERRA RODRIGUES

FUNÇÕES ARITMÉTICAS: UMA RELAÇÃO ENTRE A FUNÇÃO ϕ DE EULER E A FUNÇÃO μ DE MÖBIUS

ARAPIRACA
2019

JOSÉ ROBÉRIO BEZERRA RODRIGUES

FUNÇÕES ARITMÉTICAS: UMA RELAÇÃO ENTRE A FUNÇÃO ϕ DE EULER E A FUNÇÃO μ DE MÖBIUS

Monografia apresentada como requisito parcial para obtenção do grau de Licenciado em Matemática - Licenciatura da Universidade Federal de Alagoas - UFAL, Campus Arapiraca.

Orientador: Prof. Me. Ornan Filipe de Araújo Oliveira

Arapiraca
2019

JOSÉ ROBÉRIO BEZERRA RODRIGUES

Funções Aritméticas: uma relação entre a função ϕ de Euler e a função μ de Möbius

Monografia apresentada como requisito parcial para obtenção do grau de Licenciado em Matemática - Licenciatura da Universidade Federal de Alagoas - UFAL, Campus Arapiraca.

Data de Aprovação: 09/08/2019

Banca Examinadora

Ornan Filipe de Araujo Oliveira

Prof. Me. Ornan Filipe de Araújo Oliveira
Universidade Federal de Alagoas
Campus Arapiraca
Orientador

Rinaldo V. da S. Jr

Prof. Dr. Rinaldo Vieira da Silva Júnior
Universidade Federal de Alagoas
Campus Arapiraca
Examinador

Prof. Me. Moreno Pereira Bonutti
Universidade Federal de Alagoas
Campus Arapiraca
Examinador

AGRADECIMENTOS

Primeiramente sou grato a Deus, por mais uma conquista em minha vida.

Sou grato a minha família que tem me apoiado desde o início da minha graduação, principalmente ao meu pai e minha mãe.

Sou grato aos amigos/irmãos da minha turma da graduação, pois não poderia desejar turma melhor que a que tive. Joyce, Ana Paula, Rodrigo Costa, meus conterrâneos que estudamos juntos, meu muito obrigado. Lindinês, Janiele, Fernando e Viviane, no qual me ajudaram bastante nos estudos de Análise Real, obrigado.

Vanessa Murici, Jemerson e Sebastião os amigões da turma, vocês foram mais que importante na minha graduação. Sou muito feliz por tê-los conhecido.

Vanessa Kaline, Sheila, Priscila, Rodrigo Galdino, Lucas, Ricardo, Kelvin, Rodolfo e Alan, também, sou grato por tê-los conhecido. E por fim, agradeço aos professores do curso, por todo conhecimento que me ajudaram a adquirir, em especial, ao meu orientador Ornan e os professores Rinaldo e Moreno que me ajudaram a concluir este trabalho.

RESUMO

Este trabalho trata da Introdução a Teoria dos Números, com algumas noções preeliminares de divisibilidade, e aritmética modular como congruência, congruências lineares, e alguns teoremas clássicos, a citar os teoremas de Euler, Fermat, Wilson, e o teorema chinês dos restos. Apresentar algumas Funções Aritméticas, um conteúdo não abordado no curso de Introdução a Teoria dos Números, como a função μ de Euler, a função ϕ de Möbius e uma relação entre essas duas funções artiméticas.

Palavras-chave: Função Aritmética. Função de Euler. Função de Möbius. Congruência. Divisibilidade.

ABSTRACT

This paper presents Number Theory, with some preliminary notions of divisibility, and is modular as congruence, linear congruences, and some classical thoerems, one quoting the Euler, Fermat and wilson theorems, and the chinese remains theorem. Introduce Some Arithmetic Functions, such as Eule's μ function and Möbius φ function and a relationship between these two arithmetic funcitions.

Keywords: Arithmetic function. Euler function. Möbius function. Congruence. Divisibility.

LISTA DE SÍMBOLOS

$a \vert b$	a divide b
$a \nmid b$	a não divide b
(a, b)	o máximo divisor comum (mdc) do números a e b
$(m_1,\ m_2, \ldots,\ m_k)$	o máximo divisor comum (mdc) dos números $m_1,\ m_2, \ldots,\ m_k$
(x, y)	par ordenado de coordenadas x e y [não confundir com] (a, b)
$a \equiv b\ (\text{mod}\ m)$	a e b deixam os mesmos restos na divisão por m
$a \not\equiv b \text{mod}\ m$	a e b não deixam os mesmos restos na divisão euclidiana por m
$SCRM_{(m)}$	Sistema completo de Resíduos Módulo m
$\overline{a}$	classe de congruência "a barra"
$SRRM_{(m)}$	Sistema Reduzido de Resíduos Módulo m
$f(d)$	o valor da função f para o número d; ou simplesmente, f de d
$F(n)$	o valor da função F para o número n ou simplesmente, Fde n
$n!$	n fatorial
$E_p(n!)$	O expoente da maior potência de p que divide n fatorial
$\lfloor x \rfloor$	o maior valor inteiro de x que é menor do que ou igual a x
$\sum_{d\vert n} 1$	somar 1 para cada divisor d de n
$\sum_{d\vert n} d$	somar d para cada divisor d de n
$\sum_{d\vert n} f(d)$	somar $f(d)$ para cada divisor d de n
$\sum_{d\vert m\cdot n} f(d)$	somar $f(d)$ para cada divisor d de $m \cdot n$
$\sum_{\substack{d_1\vert m \\ d_2\vert n}} f(d_1 \cdot d_2)$	somar $f(d_1 \cdot d_2)$ sempre que d_1 divide m e d_2 divide n
$\sum_{i=1}^{n} r_i$	somatório das parcelas r_i onde i varia de 1 até n
$\prod_{i=1}^{n}$	produtório das parcelas r_i onde i varia de 1 até n
$\left(\frac{a}{p}\right)$	Símbolo de Legendre
■	marca o fim das demonstrações (como queriamos demonstrar)
♦	marca o fim dos exemplos

SUMÁRIO

1 NOÇÕES PRELIMINAR

1.1 DIVISIBILIADADE

Definição 1.1. Se a e b são inteiros, dizemos que a divide b, denotando por $a|b$, se existir um inteiro c tal que $b = ac$. Se a não divide b escrevemos $a \nmid b$.

Proposição 1.1. *Se a, b e c são inteiros, $a|b$ e $b|c$, então $a|c$.*

Demonstração. Como $a|b$ e $b|c$, existem inteiros k_1 e k_2 com $b = k_1 a$ e $c = k_2 b$. Substituindo o valor de b na equação $c = k_2 b$ teremos $c = (k_2 k_1)a$ o que implica $a|c$. ■

Exemplo 1.1. Como $3|12$ e $12|48$, então $3|48$, pois $48 = 16 \cdot 3$. Como não existe intero c satisfazendo $15 = 4 \cdot c$, então $4 \nmid 15$. ♦

Proposição 1.2. *Se a, b, c, m e n são inteiros, $c|a$ e $c|b$ então $c|(ma + nb)$.*
Demonstração. *Se $c|a$ e $c|b$ então $a = k_1 c$ e $b = k_2 c$. Multiplicando-se estas duas equações respectivamente por m e n teremos*

$$ma = mk_1 c \ \ \textbf{e} \ \ nb = nk_2 c.$$

Somando-se membro a membro obtemos

$$ma + nb = (mk_1 + nk_2 c)c \Longrightarrow c|(ma + nb).$$

■

Exemplo 1.2. Como $3|15$ e $3|42$, então $3|(8 \cdot 15 - 7 \cdot 42)$. De fato, $8 \cdot 15 - 7 \cdot 4 = 414$ e $414 = 138 \cdot 3$. ♦

Teorema 1.1. A divisão tem as seguintes propriedades:

$i)$ $n|n$

$ii)$ $d|n \Rightarrow ad|an$

$iii)$ $ad|an \Rightarrow$ e $a \neq 0 \Rightarrow d|n$

$iv)$ $1|n$

$v)$ $n|0$

$vi)$ $d|n$ e $n \neq 0 \Rightarrow |d| \leq |n|$

$vii)$ $d|n$ e $n|d \Rightarrow |d| = |n|$

$viii)$ $d|n$ e $d \neq 0 \Rightarrow \left(\frac{n}{d}\right) \mid n$

Demonstração. $i)$ Como $n = 1 \cdot n$ segue da definição 1.1 que $n|n$, inclusive para $n = 0$. Com isso demonstramos também os itens $iv)$ e $v)$.

$ii)$ Se $d|n$ então $n = cd$ para algum inteiro c. Logo $an = c(ad) \Rightarrow ad|an$. Para demonstrar $iii)$ é só fazer a volta de $ii)$. As demonstrações $vi)$ e $vii)$ são óbvias.

Demonstraremos, agora, $viii)$. Se $d|n$ então $n = k_1 d$ e portanto $\dfrac{n}{d}$ é um inteiro. Como $\left(\dfrac{n}{d}\right) \cdot d = n$ segue da definição 1.1 que $\left(\dfrac{n}{d}\right)|n$. ■

1.2 ALGORITMO DA DIVISÃO

Teorema 1.2. Sejam, $a,\ b \in \mathbb{Z},\ b > 0$. Então existem únicos $q,\ r \in \mathbb{Z}$, tal que $a = bq + r$ onde $0 \leq r < b$. Os inteiros, $a,\ b,\ q,$ e r são chamados, respectivamente, dividendo, divisor, quociente e resto.

Demonstração. Trata-se de um teorema de existência e unicidade. Enunciaresmo o chamado Princípio de Arquimiedes: Dados a e $b \in \mathbb{Z}$ com $b \neq 0$, então a é múltiplo de b ou se encontra entre dois múltiplos consecutivos de b, isto é, correspondendo a cada par de inteiros a e $b \neq 0$ existe um inteiro q tal que para $b > 0$,

$$qb \leq a \leq (q+1)b$$

para $b < 0$

$$qb \leq a \leq (q-1)b.$$

Enunciaremos o Princípio da Boa Ordem (PBO). Todo conjunto não-vazio de inteiros positivos contém um elemento mínimo.

Existência

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

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

Pelo pricípio de Arquimedes, existe $q \in \mathbb{Z}$, tal que $qb \leq a$, logo $a - qb \geq 0$ que mostra que S é não-vazio. Assim pelo PBO, existe o elemento mínimo em S que chamaremos de r. Suponhamos que $r = a - bq$, sabemos que $r \geq 0$. Vamos mostrar que $r < |b|$. Suponhamos por absurdo $r \geq |b|$. Portanto existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, logo $0 \leq s < r$. Logo, está garantida a existência de q e r.

Unicidade

Para mostrar a unicidade de q e r, suponhamos que existem q_1 e r_1 tais que

$$a = bq_1 + r_1 \qquad 0 \leq r < b$$

Então teremos

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

Por outro lado temos

$$-b < -r \leq 0 \quad \text{e} \quad 0 \leq r_1 < b$$

Isso implica

$$-b < r_1 - r < b, \text{ isto é, } |r_1 - r| < b$$

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

Corolário 1.1. *Dados dois inteiros a e b, $b \neq 0$ existem e são únicos os inteiros q e r qe satisfazem as condições*

$$a = bq + r \qquad 0 \leq r_1 < |b|$$

Demonstração. Com efeito, se $b > 0$, pelo Teorema 1.2 o resultado segue. Se $b < 0$, então $|b| > 0$, e por conseguinte existem e são únicos os inteiros q_1 e r tais que

$$a = |b|q_1 + r \qquad 0 \leq< |b|$$

Ou seja, |b|=-b

$$a = b(-q_1) + r \qquad 0 \leq r < |b|$$

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

$$a = bq + r \qquad 0 \leq r < |b|$$

■

1.3 NÚMEROS PRIMOS

Definição 1.2. Um número inteiro $n(n > 1)$ possuindo somente dois divisores positivos n e 1 é chamado *primo*.

Proposição 1.3. *Se $p|ab$, p primo, então $p|a$ ou $p|b$.*

Demonstração. Se $p \not| ab$, então $(a, p) = 1$ o que implica $p|b$. ■

Teorema 1.3. *(Teorema Fundamental da Aritmética)* Todo inteiro maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.

Demonstração. Se n é primo não há nada a ser demonstrado. Suponhamos, pois, n composto. Seja $p_1(p_1 > 1)$ o menor dos divisores positivos de n. Afirmamos que p_1 é primo. Isto é verdade, pois, caso contrário exiiria $p,\ 1 < p < p_1$ com $p|n$, contradizendo a escolha de p_1. Logo, $n = p_1 n_1$.

Se n_1 for primo a prova está completa. Caso contrário, tomamos p_2 como o menor fator de n_1. Pelo argumento anterior, p_2 é primo e temos que $n = p_1 p_2 n_2$.

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

$$n = p_1^{a_1},\ p_2^{a_2},\ \ldots, p_k^{a_k}$$

.

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

$$n = p_1 p_2 \cdots p_s$$

$$n = q_1 q_2 \cdots q_r$$

.

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

1.4 CONGRUÊNCIA

Definição 1.3. Sejam $a,\ b$ e $m \in \mathbb{Z},\ 0 \neq m$-fixo. Diremos que a é congruente a b módulo m, quando a e b deixam os mesmos restos na divisão euclidiana por m, e escreve-se:

$$a \equiv b (\text{mod } m).$$

Para indicar que a e b não são congruentes módulo m, escreve-se:

$$a \not\equiv b (\text{mod } m).$$

Teorema 1.4. Sejam $a,\ b$ e $m \in \mathbb{Z},\ 0 \neq m$-fixo. Então, $a \equiv b (\text{mod } m)$ se, e somente se, $m|(a - b)$.

Demonstração. $(\Rightarrow)$ Pelo Algoritmo da Divisão, temos:

$$a = mq_1 + r_1, \quad 0 \leqslant r_1 < |m|$$

e

$$b = mq_2 + r_2, \quad 0 \leqslant r_2 < |m|,$$

tais que $q_1,\ q_2,\ r_1$ e $r_2 \in \mathbb{Z}$.

Como $a \equiv b(\text{mod } m)$, então, pela Definição 1.3, $r_1 = r_2$. Subtraindo b de a, vem:

$$\begin{aligned} a - b &= mq_1 + r_1 - mq_2 - r_2 \\ &= m(q_1 - q_2) + r_1 - r_2 \\ &= m(q_1 - q_2) \\ &\Rightarrow m|(a - b). \end{aligned}$$

$(\Leftarrow)$ Subtraindo b de a, obtemos:

$$a - b = m(q_1 - q_2) + r_1 - r_2.$$

Como $m|(a - b)$ e é óbvio que $m(q_1 - q_2)$ é divisível por m, então $(r_1 - r_2)$ é divisível por m. Todavia, como $(r_1 - r_2) < |m|$, isto é, $-m < r_1 - r_2 < m$, então:

$$r_1 - r_2 = 0 \Rightarrow r_1 = r_2 \Rightarrow a \equiv b(\text{mod } m).$$

■

Como $m|(a-b) \Leftrightarrow |m||(a-b)$ então, nas demonstrações dos próximos teoremas, apartir daqui, limitar-nos-emos ao caso em que $m > 0$.

Demonstração. $(\Leftrightarrow)$

$$\begin{aligned} m|(a - b) &\Leftrightarrow m = (a - b)q \\ &\Leftrightarrow -m = (a - b)(-q) \\ &\Leftrightarrow -m|(a - b). \end{aligned}$$

Logo,

$$m|(a - b) \Leftrightarrow |m||(a - b).$$

■

Teorema 1.5. Sejam $a,\ b,\ c$ e $m \in \mathbb{Z},\ 0 < m$-fixo. Então, as seguintes propriedades são verdadeiras:

$i)$ $a \equiv a(\text{mod } m)$, (reflexiva);

$ii)$ $a \equiv b(\text{mod } m) \Leftrightarrow b \equiv a(\text{mod } m)$, (simétrica);

$iii)$ Se $a \equiv b(\text{mod } m)$ e $b \equiv c(\text{mod } m)$, então $a \equiv c(\text{mod } m)$, (transitiva).

Demonstração. Para provar a propriedade $i)$, basta usar a Definição 1.3, pois é óbvio que a e a deixam o mesmo resto na divisão por m. Para provar $ii)$, como $a \equiv b(\text{mod } m)$, então pelo Teorema 1.4, temos:

$$\begin{aligned} m|(a-b) &\Leftrightarrow a-b = mq \\ &\Leftrightarrow b-a = m(-q) \\ &\Leftrightarrow m|(b-a) \\ &\Leftrightarrow b \equiv a(\text{mod } m). \end{aligned}$$

Finalmente, para provarmos $iii)$, observemos que se

$$a \equiv b(\text{mod } m) \quad \text{e} \quad b \equiv c(\text{mod } m),$$

então, novamente, pelo Teorema 1.4,

$$m|(a-b) \quad \text{e} \quad m|(b-c).$$

Logo,

$$m|[(a-b)+(b-c)] \Leftrightarrow m|(a-c) \Leftrightarrow a \equiv c(\text{mod } m).$$

■

Como fica explicito no Teorema 1.5 que a relação de congruência satisfaz as propriedades reflexiva, simétrica e transitiva, então podemos afirmar que *a relação de congruência é uma relação de equivalência*.

Teorema 1.6. Sejam a e $m \in \mathbb{Z},\ 0 < m$-fixo. Então, todo inteiro a é congruente a seu resto da divisão euclidiana de a por m.

Demonstração. Pelo Algoritmo da Divisão, obtemos:

$$a = mq + r, \quad 0 \leqslant r < m \quad \Leftrightarrow$$

$$\Leftrightarrow a - r = mq \Leftrightarrow a \equiv r(\text{mod } m),$$

para únicos q e $r \in \mathbb{Z}$. ■

Em outras palavras, o Teorema 1.6 está nos dizendo que como todo inteiro a é congruente a seu resto da divisão euclidiana de a por m, então para achar o resto da divisão euclidiana de um inteiro a por m é suficiente procurar o inteiro $r \in \{0,\ 1,\ \ldots,\ m-1\}$ que seja congruente a a módulo m.

Exemplo 1.3. Para encontrar o resto da divisão de 26 por 7, por tentativas, basta procurar entre os números do conjunto $\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6\}$ o número r que satisfaz a congruência $26 \equiv r(\text{mod } 7)$ e, logo percebemos que $r = 5$, pois $26 - 5 = 7 \cdot 3$.

♦

Definição 1.4. Uma coleção de inteiros $\{a_1,\ a_2,\ \ldots,\ a_{m-1}\}$ é um *Sistema Completo de Resíduos Módulos* m $(SCRM_{(m)})$, quando cada inteiro é congruente módulo m a um único inteiro a_i, $i \in \{1,\ 2,\ \ldots,\ m-1\}$ e dois quaisquer destes a_i não são congruentes módulo m.

Em símbolos, a Definição 1.4 se expressa assim:

$\{a_1,\ \ldots,\ a_{m-1}\}$ é $SCRM_{(m)} \Leftrightarrow$

$$\begin{cases} \exists!\ i \in \{1,\ \ldots,\ m-1\}\ ;\ n \equiv a_i (\text{mod}\ m),\ \forall\ n \in \mathbb{Z}, \\ \text{e} \\ i \neq j \Leftrightarrow a_i \not\equiv a_j (\text{mod}\ m), \forall\ i,\ j \in \{1,\ \ldots,\ m-1\}. \end{cases}$$

Teorema 1.7. Sejam a e $m \in \mathbb{Z},\ 0 < m$-fixo. Se o conjunto $\{0,\ 1,\ \ldots,\ m-1\}$ é o conjunto dos possíveis restos da divisão euclidiana da a por m, então dois quaisquer desses restos não são congruentes módulo m.

Demonstração. Utililizaremos o método de redução ao absurdo.

Sejam $a_i = m - i$ e $a_j = m - j$ elementos do conjunto $\{0,\ 1,\ \ldots,\ m-1\}$, tais que $i \neq j$ e $i,\ j \in \{1,\ \ldots,\ m\}$. Suponhamos por absurdo que $a_i \equiv a_j (\text{mod}\ m)$. Daí,

$$(m-i) \equiv (m-j)(\text{mod}\ m).$$

Mas, pelo Teorema 1.4, obtemos:

$$m|[(m-i)-(m-j)] \Leftrightarrow m|(i-j). \text{ Absurdo!}$$

Pois, $i \neq j$ e

$$\begin{cases} 1 \leqslant i \leqslant m & (-L_1) \\ 1 \leqslant j \leqslant m & (L_2) \end{cases} \approx \begin{cases} -m \leqslant -i \leqslant -1 & (L_3) \\ 1 \leqslant j \leqslant m & (L_2+L_3) \end{cases} \approx$$

$$\approx \begin{cases} -m \leqslant -i \leqslant -1 \\ -(m-1) \leqslant j-i \leqslant m-1 \end{cases} \Rightarrow j - i \leqslant |m-1| \Rightarrow 0 \neq j-i < |m|,$$

todavia, o único número divisível por $|m|$ menor do que $|m|$ é o zero.

Logo, no conjunto $\{0,\ 1,\ \ldots,\ m-1\}\}$ dois quaisquer de seus elementos não são congruentes módulo m. ■

Corolário 1.2. *O conjunto* $\{0,\ 1,\ \ldots,\ m-1\}$ *é um* $SCRM_{(m)}$.

Demonstração. Sejam $a,\ m \in \mathbb{Z},\ a$-arbitrário e $0 < m$-fixo. Então, pelo Algoritmo da Divisão existem únicos $q,\ r \in \mathbb{Z}$, tais que:

$$a = mq + r.$$

Como $r \in \{0,\ 1,\ \ldots,\ m-1\}$ e pelo Teorema 1.7 dois quaisquer desses restos não são congruentes módulo m, então existe um único $r \in \{0,\ 1,\ \ldots,\ m-1\}$ tal que

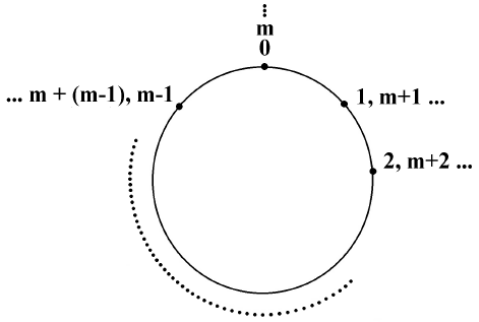
$$a \equiv r(\text{mod}\ m),\ \ \forall\ a \in \mathbb{Z}.$$

Logo, pela Definição 1.4 o conjunto $\{0,\ 1,\ \ldots,\ m-1\}$ é um $SCRM_{(m)}$. ■

Em outras palavras, o Corolário 1.2 está nos dizendo que a relação de congruência separa os inteiros em classes de equivalência módulo m, isto é, os inteiros de uma classe são aqueles congruentes módulo m.

Geometricamente, com uma circunferência dividida em m partes, fazemos corresponder a cada ponto assinalado um dos elementos do conjunto $\{0,\ 1,\ \ldots,\ m-1\}$, como na figura abaixo:

Figura 1



Fonte: MILIES. p. 105.

Portanto, em termos geométricos, a Definição 1.3 nos afirma que dois inteiros são congruentes módulo m se, e somente se, estes inteiros são representados pelo mesmo ponto da circunferência supramencionada, ou seja, cada ponto pode ser interpretado como uma classe de equivalência módulo m.

Teorema 1.8. Se $R = \{r_0,\ r_1,\ \ldots,\ r_k\}$ é um $SCRM_{(m)}$, então $k = m$.

Demonstração. Como pelo Corolário 1.2, o conjunto $T = \{t_0,\ t_1,\ \ldots,\ t_{m-1}\}$ é um $SCRM_{(m)}$, para $t_i = i = 0,\ 1,\ \ldots,\ m-1$, então garantimos que cada r_i é congruente a exatamente um dos t_i, isto é, $k \leqslant m$. Por outro lado, como R é um $SCRM_{(m)}$, então cada t_i é congruente a exatamente um dos r_i, ou seja, $m \leqslant k$.

Logo, como $k \leqslant m$ e $m \leqslant k$, então $m = k$. ■

Teorema 1.9. Sejam $a,\ b,\ c,\ m \in \mathbb{Z},\ 0 < m$-fixo. Tem-se que

$$a \pm c \equiv b \pm c (\text{mod } m) \Leftrightarrow a \equiv b (\text{mod } m).$$

Demonstração. De fato,

$$\begin{aligned} a \pm c \equiv b \pm c (\text{mod } m) &\Leftrightarrow m|[(a \pm c) - (b \pm c)] \\ &\Leftrightarrow m|(a-b) \\ &\Leftrightarrow a \equiv b (\text{mod } m). \end{aligned}$$

■

Teorema 1.10. Sejam $a,\ b,\ c,\ m \in \mathbb{Z},\ c > 0$ e $1 < m$-fixo. Se $a \equiv b(\text{mod } m)$, então

$$ac \equiv bc(\text{mod } cm)$$

e a recíproca é veredadeira.

Demonstração. Com efeito,

$$\begin{aligned} a \equiv b(\text{mod } m) &\Leftrightarrow m|(a-b) \\ &\Leftrightarrow a - b = mq,\ \ q \in \mathbb{Z}. \end{aligned}$$

Multiplicando a última equação por $c > 0$, vem:

$$\begin{aligned} c(a-b) = c(mq) &\Leftrightarrow ca - cb = (cm)q \\ &\Leftrightarrow (cm)|(ca-cb) \\ &\Leftrightarrow (cm)|(ac-bc) \\ &\Leftrightarrow ac \equiv bc(\text{mod } cm) \end{aligned}$$

■

Teorema 1.11. Sejam $a,\ b,\ m$ e $n \in \mathbb{Z}$, com $0 < n,$ e $0 < m$-fixo. Se $a \equiv b(\text{mod } m)$ e $n|m$, então $a \equiv b(\text{mod } n)$.

Demonstração. Como, pelo Teorema 1.4, $m|(a-b)$ e $n|m$, então por transitividade $n|(a-b)$ e, portanto, $a \equiv b(\text{mod } n)$. ■

Teorema 1.12. Sejam $a,\ b,\ m \in \mathbb{Z},\ 1 < m$-fixo. Se $a \equiv b(\text{mod } m)$, então $(a, m) = (b, m)$.

Demonstração. Lembremos que

$i)$ Se $a,\ b$ e $m \in \mathbb{Z}$ e $b = a + mq$, então $(a, m) = (b, m)$.

Como $a \equiv b(\text{mod } m)$, então pelo Teorema 1.4, $m|(a-b)$, isto é, $b - a = mq$ e, portanto, $b = a + mq,\ q \in \mathbb{Z}$. Logo, pelo item $i)$ acima, obemos:

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

■

Teorema 1.13. Sejam $a,\ b,\ c,\ d$ e $m \in \mathbb{Z},\ 0 < m$-fixo. Se $a \equiv b(\text{mod } m)$ e $c \equiv d(\text{mod } m)$, então:

$i)$ $a \pm c \equiv b \pm d(\text{mod } m)$

$ii)$ $ac \equiv bd(\text{mod } m)$.

Demonstração. Para provar $i)$, como $a \equiv b(\text{mod } m)$ e $c \equiv d(\text{mod } m)$ então, pelo Teorema 1.4, $m|(a-b)$ e $m|(c-d)$. Logo,

$$m|[(a-b) \pm (c-d)] \Leftrightarrow m|[(a \pm c) - (b \pm d)]$$
$$\Leftrightarrow a \pm c \equiv b \pm d(\text{mod } m).$$

Para provar $ii)$, como $a \equiv b(\text{mod } m)$ e $c \equiv d(\text{mod } m)$, então, novamente pelo Teorema 1.4, obtemos:

$$a - b = mq_1 \Leftrightarrow a = b + mq_1$$
$$c - d = mq_2 \Leftrightarrow c = d + mq_2.$$

Daí,

$$\begin{aligned} ac &= (b + mq_1)(d + mq_2) \\ &= bd + bmq_2 + mq_1d + m^2q_1q_2 \\ &= bd + m(bq_2 + q_1d + mq_1q_2). \end{aligned}$$

Portanto,

$$ac - bd = m(bq_2 + q_1d + mq_1q_2) \Leftrightarrow m|(ac - bd) \Leftrightarrow ac \equiv bd(\text{mod } m)$$

■

Corolário 1.3. *Sejam* $a,\ b,\ m \in \mathbb{Z},\ 0 < m$*-fixo e* $n \in \mathbb{Z}_+^*$. *Se* $a \equiv b($*mod* $m)$, *então* $a^n \equiv b^n($*mod* $m)$.

Demonstração. Usaremos o Princípio da Indução Finita (PIF) sobre n.

Seja $X = \{n \in \mathbb{Z}_+^*;\ a^n \equiv b^n(\text{mod } m)\}$. Por hipótese, $1 \in X$ pois, $a^1 \equiv b^1(\text{mod } m)$.

Suponhamos que $k \in X$, isto é, $a^k \equiv b^k(\text{mod } m)$ com $k \in \mathbb{Z}_+^*$. *Hipótese de Indução* (H.I.). Queremos mostrar que $(k+1) \in X$, isto é, $a^{k+1} \equiv b^{k+1}(\text{mod } m)$.

De fato, como $a \equiv b(\text{mod } m)$ e $\underbrace{a^k \equiv b^k(\text{mod } m)}_{\text{H.I.}}$, acarreta, pelo item $ii)$ do Teorema 1.13, que:

$$a \cdot a^k \equiv b \cdot b^k(\text{mod } m) \Leftrightarrow a^{k+1} \equiv b^{k+1}(\text{mod } m).$$

Logo, $k+1 \in X$.

Portanto, pelo PIF $X = \mathbb{Z}_+^*$, isto é, $a^n \equiv b^n(\text{mod } m),\ \forall\ n \in \mathbb{Z}_+^*$. ■

Corolário 1.4. *Sejam* $a,\ b,\ m \in \mathbb{Z},\ 0 < m$*-fixo. Se* $a+b \equiv 0($*mod* $m)$, *então para todo* $n \in \mathbb{Z}_+^*$, *tem-se que*

$$a^{2n} \equiv b^{2n}(\textit{mod } m) \quad \textit{e} \quad a^{2n+1} + b^{2n+1} \equiv 0(\textit{mod } m).$$

Demonstração. Como $a + b \equiv 0(\text{mod } m)$, então $m|(a+b)$ e, consequentemente, $m|[(a+b)(a-b)] \Leftrightarrow m|(a^2 - b^2)$, isto é, $a^2 \equiv b^2(\text{mod } m)$. Aplicando o Corolário 1.3, obtemos:

$$(a^2)^n \equiv (b^2)^n(\text{mod } m) \Leftrightarrow$$

$$a^{2n} \equiv b^{2n} (\text{mod } m). \tag{1.1}$$

Por outro lado, como é óbvio que pela Definição 1.3 $-b \equiv -b (\text{mod } m)$ e, por hipótese, $a + b \equiv 0 (\text{mod } m)$, então pelo item $i)$ do Teorema 1.13 podemos somar estas congruências, o que acarreta em:

$$a \equiv -b (\text{mod } m). \tag{1.2}$$

Pelo item $ii)$ do Teorema 1.13 podemos multiplicar a congruência 1.1 pela congruência 1.2 o que resulta em:

$$a^{2n+1} \equiv -b^{2n+1} (\text{mod } m). \tag{1.3}$$

E finalmente, como pela Definição 1.3 $b^{2n+1} \equiv b^{2n+1} (\text{mod } m)$, então pelo item $i)$ do Teorema 1.13 podemos somar esta congruência com a congruência 1.3 para obtermos:

$$\begin{aligned} a^{2n+1} + b^{2n+1} &\equiv -b^{2n+1} + b^{2n+1} (\text{mod } m) \\ a^{2n+1} + b^{2n+1} &\equiv 0 (\text{mod } m). \end{aligned}$$

■

Teorema 1.14. Sejam $a,\ b,\ c,\ m \in \mathbb{Z},\ 0 < m$-fixo. Então, é verdade que

$$ac \equiv bc (\text{mod } m) \Rightarrow a \equiv b \left(\text{mod } \left(\frac{m}{(c, m)} \right) \right),$$

onde (m, c) é o *máximo divisor comum* de m e c.

Demonstração. Lembremos que

$i)$ Se (a, b) é o máximo divisor comum entre a e b, então $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)} \right) = 1.$

$ii)$ Se $a|bc$ e $(a, b) = 1$, então $a|c$.

Por hipótese,

$$\begin{aligned} ac \equiv bc (\text{mod } m) &\Leftrightarrow m|(ac - bc) \\ &\Leftrightarrow m|(a - b)c \\ &\Leftrightarrow \left(\frac{m}{(m,c)} \right) | (\, a - b) \left(\frac{c}{(m,c)} \right). \end{aligned}$$

Mas, pelo item $i)$ acima

$$\left(\left(\frac{m}{(m,c)} \right), \left(\frac{c}{(m,c)} \right) \right) = 1.$$

Então,

$$\left(\frac{m}{(m,c)} \right) \nmid \left(\frac{c}{(m,c)} \right).$$

Logo, pelo item $ii)$ acima, vem:

$$\left(\frac{m}{(m,c)}\right) \mid (a-b),$$

ou seja,

$$a \equiv b \left(\text{mod } \left(\frac{m}{(m-c)}\right)\right).$$

■

Corolário 1.5. *Sejam* $a,\ b,\ c$ *e* $m \in \mathbb{Z}$, $0 < m$*-fixo. Se* $ac \equiv bc$(*mod* m) *e* $(m,c) = 1$ *então,* $a \equiv b$(*mod* m).

Demonstração. De fato, por hipótese:

$$m|(ac-bc) \Leftrightarrow m|(a-b)c$$
$$\Leftrightarrow \left(\frac{m}{(m,c)}\right)|(\,a-b)\left(\frac{c}{(m,c)}\right).$$

Como $\left(\left(\frac{m}{(m,c)}\right), \left(\frac{c}{(m,c)}\right)\right) = 1,$ então $\left(\frac{m}{(m,c)}\right) \nmid \left(\frac{c}{(m,c)}\right).$

Logo, como $\frac{m}{(m,c)} = \frac{m}{1} = m,$ então

$$m|(a-b) \Leftrightarrow a \equiv b(\text{mod } m).$$

■

Teorema 1.15. Sejam $a,\ b \in \mathbb{Z},\ m_i$-fixo $\in \mathbb{Z}_+ - \{1\},\ i = 1,\ 2,\ \ldots,\ k$, tal que $k \in \mathbb{Z}_+ - \{1\}$. Se $a \equiv b(\text{mod } m_i)$, então:

$$a \equiv b(\text{mod } [m_1,\ m_2,\ \ldots,\ m_k]),$$

onde $[m_1,\ m_2,\ \ldots,\ m_k]$ é o *mínimo múltiplo comum* dos números $m_1,\ m_2,\ \ldots,\ m_k$.

Demonstração. Lembremos que:

$i)$ $a|b^n \Leftrightarrow a|b,\ n \in \mathbb{Z}$;

$ii)$ Sejam $a = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_n^{a_n},\ b = p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_n^{b_n},\ \ldots,\ h = p_1^{h_1} \cdot p_2^{h_2} \cdot \ldots \cdot p_n^{h_n}$ inteiros tais que $p_1,\ p_2,\ \ldots,\ p_n$ são os primos das fatorações de $a,\ b,\ \ldots,\ h$ então:

$$[a,\ b,\ \ldots,\ h] = p_1^{\max\{a_1,\ b_1,\ \ldots,\ h_1\}} \cdot p_2^{\max\{a_2,\ b_2 \cdots h_2\}} \cdots p_n^{\max\{a_n,\ b_n,\ \ldots,\ h_n\}}$$

(nas fatorações dos inteiros $a,\ b,\ \ldots,\ h$ podem existir expoentes nulos, para os $p_j's$, $j = 1,\ 2,\ \ldots,\ n$);

$iii)$ A divisão é transitiva, isto é, se $a|b$ e $b|c$, então $a|c$ tal que $a,\ b,\ c \in \mathbb{Z}^*$.

Seja p_n o maior primo que aparece nas fatorações dos $m_i,\ i = 1,\ 2,\ \ldots,\ k$. Então, pelo *Teorema Fundamental da Aritmética* (TFA), cada m_i pode ser expresso como

$$m_i = p_1^{\alpha_{1i}} \cdot p_2^{\alpha_{2i}} \cdot \ldots \cdot p_n^{\alpha_{ni}},$$

onde para $p_j,\ j = 1,\ 2,\ \ldots,\ n$, pode existir $\alpha_{ji} = 0$.

Por transitividade (item iii) acima), como $m_i|(a-b)$, então $p_j{}^{\alpha_{ji}}|(a-b),\ i = 1,\ 2,\ \ldots,\ k$ e $j = 1,\ 2,\ \ldots,\ n$.

Como

$$\begin{aligned} m_1 &= p_1^{\alpha_{11}} \cdot p_2^{\alpha_{21}} \cdot \ldots \cdot p_n^{\alpha_{n1}} \\ m_2 &= p_1^{\alpha_{12}} \cdot p_2^{\alpha_{22}} \cdot \ldots \cdot p_n^{\alpha_{n2}} \\ \vdots &\qquad\qquad \vdots \\ m_k &= p_1^{\alpha_{1k}} \cdot p_2^{\alpha_{2k}} \cdot \ldots \cdot p_n^{\alpha_{nk}}, \end{aligned}$$

então tomemos $\alpha_j = \max\limits_{1 \leqslant i \leqslant k}\{\alpha_{ji}\}$ e como $p_j{}^{\alpha_{ji}}|(a-b),\ i = 1,\ 2,\ \ldots,\ k$ e $j = 1,\ 2,\ \ldots,\ n$, teremos que

$$\begin{aligned} p_1^{\alpha_1} \cdot q_1 &= a - b \\ p_2^{\alpha_2} \cdot q_2 &= a - b \\ \vdots &\qquad \vdots \\ p_n^{\alpha_n} \cdot q_n &= a - b. \end{aligned}$$

Multipliquemos as n equações acima, membro a membro, para obter:

$$\begin{aligned} (a-b)^n &= (q_1 \cdot q_2 \cdot \ldots q_n)(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha^n}) \\ &\Leftrightarrow (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n})|(a-b)^n \\ &\Leftrightarrow (p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n})|(a-b), \end{aligned}$$

onde a última dupla implicação é verdadeira por causa do item $i)$ acima. Todavia, pelo item $ii)$ acima

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n} = [m_1,\ m_2,\ \ldots,\ m_k].$$

Portanto,

$$[m_1,\ m_2,\ \ldots,\ m_k]|(a-b) \Leftrightarrow a \equiv b(\text{mod } [m_1,\ m_2,\ \ldots,\ m_k]).$$

■

Teorema 1.16. Sejam $a,\ b$ e $m \in \mathbb{Z},\ 0 < m$-fixo e $(b, m) = 1$. Se o conjunto $A = \{a_0,\ \ldots,\ a_{m-1}\}$ é um $SCRM_{(m)}$, então o conjunto $B = \{a + ba_0,\ \ldots,\ a + ba_{m-1}\}$, também, é um $SCRM_{(m)}$.

Demonstração. Inicialmente, usaremos o *Método de Redução ao Absurdo* (MRA).

Suponhamos $a + ba_i \equiv a + ba_j(\text{mod } m),\ i \neq j$, para $i,\ j \in M = \{0,\ 1,\ \ldots,\ m-1\}$. Do Teorema 1.9, obtemos:

$$a + ba_i \equiv a + ba_j(\text{mod } m) \Leftrightarrow ba_i \equiv ba_j(\text{mod } m).$$

E do Corolário 1.5, temos:

$$ba_i \equiv ba_j(\text{mod } m) \Leftrightarrow a_i \equiv a_j(\text{mod } m). \text{ Absurdo!}$$

Pois, para $i \neq j$, quaisquer elementos do conjunto $A = \{a_0, \ \ldots, \ a_{m-1}\}$ são dois a dois incongruentes módulo m, isto é, $a_i \not\equiv a_j(\text{mod } m)$.

Além disso, como o conjunto A é um $SCRM_{(m)}$ e em B acabamos de verificar pelo (MRA) que $a + ba_i \not\equiv a + ba_j(\text{mod } m),$ para $i \neq j$, e tanto em A quanto em B existem m elementos, então para todo elemento $a_i \in A$ existe um único elemento correspondente $(a + ba_h) \in B, \ h \in M$, tal que $a_i \equiv a + ba_h(\text{mod } m)$ e, logo, existe um único $(a + ba_h) \in B$, tal que

$$k \equiv a + ba_h(\text{mod } m), \ \ \forall k \in \mathbb{Z}.$$

Portanto, pela Definição 1.4, B é um $SCRM_{(m)}$. ■

Definição 1.5. Sejam $a, \ b, \ q$ e $m \in \mathbb{Z}, \ 1 < m$-fixo e $b = a + mq$. Diremos que o seguinte conjunto $\overline{a} = \{a + mq; \ q \in \mathbb{Z}\} = \{b \in \mathbb{Z}; \ b \equiv a(\text{mod } m)\}$ é *a classe de equivalência* $\overline{a}$ *dos* b *inteiros congruentes para* a *módulo* m (classe de congruência $\overline{a}$), isto é, o conjunto dos b inteiros que na divisão euclidiana por m deixam resto a.

Seja $a \in \mathbb{Z}, \ r \in \{0, \ 1, \ \ldots, \ m-1\}$. Se $a \equiv r(\text{mod } m)$, pelo Teorema 1.6, r é único e, consequentemente, a pertence a uma única das seguintes classes de congruência:

$$\overline{0}, \ \overline{1}, \ \ldots, \ \overline{m-1}.$$

Portanto, qualquer conjunto de elementos representativos (um de cada uma destas classes) é chamado um $SCRM_{(m)}$. Em símbolos, dado um único $r_i \in \overline{i}, \ i \in \{0, \ 1, \ \ldots, m-1\}$, tem-se que:

$$R = \{r_i \in \overline{i}; \ 0 \leqslant i \leqslant m-1\}$$

é um $SCRM_{(m)}$.

1.5 CONGRUÊNCIA LINEAR

Definição 1.6. Dizemos que a congruência $ax \equiv b(\text{mod } m)$ é uma congruência linear em uma variável, quando x é uma incógnita.

Teorema 1.17. Sejam x_0 e $x_1 \in \mathbb{Z}$. Se x_0 é um solução à congruência $ax \equiv b(\text{mod } m)$, isto é, $ax_0 \equiv b(\text{mod } m)$, e $x_1 \equiv x_0(\text{mod } m)$, então x_1, também, é solução à congruência $ax \equiv b(\text{mod } m),$ ou seja, $ax_1 \equiv b(\text{mod } m)$.

Demonstração. Como $ax_0 \equiv b(\text{mod } m)$, e $x_1 \equiv x_0(\text{mod } m)$ se, e somente se, $ax_1 \equiv ax_0(\text{mod } m)$, então por transitividade (Teorema 1.5 item iii)), acarreta que:

$$ax_1 \equiv ax_0 \equiv b(\text{mod } m).$$

■

Em outras palavras, o Teorema 1.17 nos garante que se um elemento representativo de uma classe de equivalência $\overline{a}$ é solução para uma congruência linear, então todos os representantes de $\overline{a}$, também, são soluções.

Daí aparece uma importante questão: quando uma congruência linar tem mais do que uma solução, quantas destas soluções são incongruentes?

Para ter condições de responder esta questão, primeiro teremos que demonstrar um teorema que nos fornece informações concernentes à existência de soluções para uma *equação diofantina*.

Definição 1.7. Dizemos que uma equação linear do tipo $ax + by = c$ é uma *equação linear diofantina* quando $a,\ b$ e $c \in \mathbb{Z}$, e a e b não são ambos nulos. Logo, as soluções para este tipo de equação são pares ordenados de inteiros (x, y).

O nome de tais equações é em homenagem ao matemático grego Diofanto de Alexandria que foi o primeiro a se preocupar com problemas deste tipo (em torno de 250 d.C.), ou seja, com equações indeterminadas que ocasionalmente tem infinitas soluções; porém ele procurava soluções racionais, isto é, pares (x, y) tais que $x,\ y \in \mathbb{Q}$.

Teorema 1.18. Sejam $a,\ b,\ d,\ x$ e $y \in \mathbb{Z}$, tais que $(a, b) = d,\ a,\ b$-fixos e, $x,\ y$-incógnitas. Se $d \nmid c$, então a equação $ax + by = c$ não tem solução inteira. Mas, se $d|c$, então esta equação tem infinitas soluções. Além disso, se (x_0, y_0) é uma solução particular, então todas as soluções são dadas por

$$x = x_0 + (b/d)k$$
$$y = y_0 - (a/d)k, \quad k \in \mathbb{Z}.$$

Demonstração. Sejam $a,\ b,\ \alpha,\ \beta,$ e $d \in \mathbb{Z},\ d \neq 0$. Lembremos que:

i) se $d|a$ e $d|b$, então $d|(a\alpha + b\beta)$;

ii) se $(a, b) = d$, então exitem α e β tais que $a\alpha + b\beta = d$.

Inicialmente, provaremos que toda solução da equação $ax + by = c$ é dada por $x = x_0 + (b/d)k,\ y = y_0 - (a/d)k$. Seja (x, y) uma solução, isto é,

$$ax + by = c. \tag{1.4}$$

Suponhamos que $(x_0,\ y_0)$, também, é solução, ou seja:

$$ax_0 + by_0 = c. \tag{1.5}$$

Então, subtraiamos a equação 1.5 da equação 1.4, membro a membro, para obtermos:

$$ax + by - ax_0 - by_0 = a(x - x_0) + b(y - y_0) = 0$$
$$\Leftrightarrow a(x - x_0) = b(y_0 - y).$$

Como $(a, b) = d$, então lembremos que:

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Logo, dividamos o 1^o e o 2^o membro da última igualdade por d para conseguirmos:

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y.) \tag{1.6}$$

Portanto, note que na equação 1.6, necessariamente, $\frac{b}{d}|(x - x_0)$ e $\frac{a}{d}|(y_0 - y)$, isto é:

$$x - x_0 = k(b/d) \Leftrightarrow x = x_0 + k(b/d) \tag{1.7}$$

e

$$y_0 - y = k(a/d) \Leftrightarrow y = y_0 - k(a/d), \;\; k \in \mathbb{Z}. \tag{1.8}$$

Agora, anlisemos a existência das soluções à equação $ax + by = c$.

Se $d \nmid c$, então $d \nmid (ax + by)$. Absurdo! Pois, como $(a, b) = d$, então d divide qualquer combinação linear de a e b (item i) acima), inclusive a combinação $ax + by$. Logo, se $d \nmid c$, com efeito, não existem x e y tais que $ax + by = c$ é satisfeita, isto é, *não há solução à equação* $ax + by = c$.

Se $d|c$, então $c = kd, \; k \in \mathbb{Z}$. Como $(a, b) = d$, então, pelo item $ii)$ acima existem α e β tais que

$$a\alpha + b\beta = d. \tag{1.9}$$

Multipliquemos, a equação 1.9 pelo inteiro k, para obtermos:

$$a(\alpha k) + b(\beta k) = kd = c. \tag{1.10}$$

Note que a equação 1.10 expressa que o par ordenado $(x_0, \; y_0), \;$ com $x_0 = \alpha k$ e $y_0 = \beta k$, é uma solução para $ax + by = c$. Investiguemos se isto é verdade com as equações 1.7 e 1.8. Logo,

$$x = x_0 + (b/d)k$$
$$y = y_0 - (a/d)k.$$

Daí,

$$\begin{aligned} ax + by &= a(x_0 + (b/d)k) + b(y_0 - (a/d)k) \\ &= ax_0 + \frac{ab}{d}k + by_0 - \frac{ab}{d}k \\ &= ax_0 + by_0 \\ &= c. \end{aligned}$$

Portanto, se soubermos uma solução particular (x_0, y_0), então a partir dela podemos gerar infinitas soluções, com as equações

$$x = x_0 + (b/d)k$$
$$y = y_0 - (b/d)k.$$

■

Agora, de posse do Teorema 1.18 poderemos dizer quantas soluções incongruentes a congruência $ax \equiv b(\text{mod } m)$ tem, caso exista alguma.

Teorema 1.19. Sejam $a,\ b,$ e $m \in \mathbb{Z}$, tais que $0 < m$ e $(a, m) = d$. Se $d \nmid b$, então a congruência $ax \equiv b(\text{mod } m)$ não tem solução, mas quando $d|b$, então esta congruência tem exatamente d soluções incongruentes módulo m.

Demonstração. Lembremos que:

$i)$ Sejam $\alpha,\ \beta \in \mathbb{Z},\ \alpha \neq 0$. Se $\alpha|\beta,$ então $(\beta/\alpha)|\beta$.

Pelo Teorema 1.4, x é solução de $ax \equiv b(\text{mod } m)$ se, e somente se,

$$\begin{aligned} m|(ax - b) &\Leftrightarrow ax - b = my \\ &\Leftrightarrow ax = b + my \\ &\Leftrightarrow ax - my = b, \end{aligned}$$

para $x,\ y \in \mathbb{Z}$.

Do Teorema 1.18 é sabido que a equação $ax - my = b$ não tem solução se $d \nmid b$, e que ela tem infinitas soluções se $d|b$, dadas por $x = x_0 + (b/d)k$ e $y = y_0 - (a/d)k,$ ou seja, (x_0, y_0) é uma solução particular para $ax - my = b$. Daí, equivalentemente, a congruência $ax \equiv b(\text{mod } m)$ tem um infinidade de soluções do tipo $x = x_0 + (\frac{m}{d})k$.

Como é de nosso propósito saber o número de soluções incongruentes, analisaremos quais são as condições em que $x_1 = x_0 + (m/d)k_1$ e $x_2 = x_0 + (m/d)k_2$ são congruentes módulo m. Assim, suponhamos que x_1 e x_2 são congruentes, ou melhor,

$$x_0 + (m/d)k_1 \equiv x_0 + (m/d)k_2(\text{mod } m) \Leftrightarrow (m/d)k_1 \ \equiv (m/d)k_2(\text{mod } m),$$

mas como $d|m$, pelo item $i)$ acima, então $(m/d)|m$ e, logo $(m/d, m) = m/d$. Portanto, pelo Teorema 1.14

$$\begin{aligned} (m/d)k_1 \equiv (m/d)k_2(\text{mod } m) &\Leftrightarrow k_1 \equiv k_2 \left(\text{mod } \frac{m}{(m/d)}\right) \\ &\Leftrightarrow k_1 \equiv k_2(\text{mod } d). \end{aligned}$$

Note que, pela Definição 1.5, k_1 e k_2 são elementos representativos da mesma classe de equivalência módulo d.

Logo, se $d|b$ e $(a, m) = d$, para uma congruência linear de uma váriável $ax \equiv b(\text{mod } m)$ temos exatamente d soluções incongruentes do tipo $x = x_0 + (m/d)k$, onde k percorre o $SCRM_{(d)} = \{1,\ 2,\ \ldots,\ d\}$. ∎

Definição 1.8. Dizemos que uma solução x_0 de $ax \equiv b(\text{mod } m)$ é única módulo m quando qualquer outra solução x_1 for congruente a x_0 módulo m.

Definição 1.9. Uma solução $\overline{b}$ de $ax \equiv 1(\text{mod } m)$ é chamada de um *inverso* de a módulo m.

Note que é imediato, pelo Teorema 1.19, que de acordo com a definição 1.9, se $(a, m) = 1$, então o inverso de a é único.

Teorema 1.20. Sejam $a,\ p \in \mathbb{Z},\ p$-primo. Então, a é seu próprio inverso módulo m se, e somente se, $a \equiv 1(\text{mod } p)$ ou $a \equiv -1(\text{mod } p)$.

Demonstração. $(\Leftrightarrow)$ Se a é seu próprio inverso, então $a^2 \equiv 1(\text{mod } p)$, pelo Teorema 1.4 se, somente se:

$$\begin{aligned} m|(a^2-1) &\Leftrightarrow p|(a-1)(a+1) \\ &\Leftrightarrow p|(a-1) \text{ ou } p|(a+1) \\ &\Leftrightarrow a \equiv 1(\text{mod } p) \text{ ou } a \equiv -1(\text{mod } p). \end{aligned}$$

■

1.6 OS TEOREMAS DE EULER, FERMAT E WILSON

Teorema 1.21. (Teorema de Wilson): Se p-primo $\in \mathbb{Z}_+$, então $(p-1)! \equiv -1(\text{mod } p)$.

Demonstração. Pelo Teorema 1.19, a congruência $ax \equiv 1(\text{mod } p)$ tem uma única solução para $a \in P = \{0,\ 1,\ 2,\ \ldots,\ p-1\}$. Por outro lado, pelo Teorema 1.20, em P há apenas o elemento 1 e o elemento $(p-1)$ que são seus próprios inversos módulo p. Então, é evidente que só podemos formar $(p-3)/2$ pares com os números restantes $2,\ 3,\ \ldots$ e $(p-2)$, cujo o produto é congruente a 1 módulo p. Isto porquanto, pelo item $ii)$ do Teorema 1.13, podemos multiplicar tais congruências uma pela outra, membro a membro sucessivamente, para obtermos:

$$2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-3) \cdot (p-2) \equiv 1(\text{mod } p) \tag{1.11}$$

Agora, multipliquemos a congruência 1.11 com $p - 1 \equiv p - 1(\text{mod } p)$, membro a membro, para gerarmos:

$$2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-3) \cdot (p-2) \cdot (p-1) \equiv (p-1)(\text{mod } p).$$

Logo, como $p - 1 \equiv -1(\text{mod } p)$, então por transitividade:

$$\begin{aligned} 2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-3) \cdot (p-2) \cdot (p-1) &\equiv (p-1)(\text{mod } p) \\ &\equiv -1(\text{mod } p) \\ &\Leftrightarrow (p-1)! \equiv -1(\text{mod } p). \end{aligned}$$

■

Teorema 1.22. Se n é um inteiro tal que $(n-1)! \equiv -1(\text{mod } n)$, então n é primo.

Demonstração. Usaremos o *Método de Redução ao Absurdo* (MRA).

Suponhamos que $(n-1)! \equiv -1(\text{mod } n)$ e que n não é primo. Logo, $n = kq$ com $1 < k < n$ e $1 < q < n,$ onde $k,\ q \in \mathbb{Z}$. Nestas condições, note que tanto $k|(n-1)!$, quanto

$q|(n-1)!$. Como $n|((n-1)!+1),\ k|n$ e $q|n$, por transitividade, então

$$k|[(n-1)!+1] \text{ e } q|[(n-1)!+1] \Rightarrow k|[(n-1)!+1-(n-1)!] \text{ e } q|[(n-1)!+1-(n-1)!]$$
$$\Rightarrow k|1 \text{ e } q|1. \text{ Absurdo!}$$

Pois, $1 < k$ e $1 < q$.

Portanto, se $(n-1)! \equiv -1(\text{mod } n)$, então n é primo. ■

Teorema 1.23. (Pequeno Teorema de Fermat): Sejam $a, p \in \mathbb{Z}$, com p-primo, tal que $p \nmid a$. Então,

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

Demonstração. Como $p \nmid a$ e p é primo, então $a \neq 0$ e $(a,p) = 1$. Consideremos o seguinte conjunto

$$A = \{b + ia;\ b = 0 \text{ e } 0 \leqslant i \leqslant p-1\} = \{0,\ a,\ \ldots,\ (p-1)a\}.$$

Como pelo Corolário 1.2 o conjunto $B = \{0,\ \ldots,\ p-1\}$ é um $SCRM_{(p)}$, então pelo Teorema 1.16 o conjunto A, também, é um $SCRM_{(p)}$. Daí, o conjunto

$$A - \{0\} = \{a,\ 2a,\ \ldots,\ (p-1)a\}$$

preserva o fato de que seus elementos são incongruentes dois a dois, embora não seja um $SCRM_{(p)}$, haja vista a forma como o construimos.

Como no conjunto $B - \{0\} = \{1,\ 2,\ \ldots,\ p-1\}$ seus elementos são incongruentes dois a dois, então os elementos de $A - \{0\}$ são congruentes aos elementos de $B - \{0\}$, numa ordem conveniente. Isto é, temos $p-1$ congruências da forma:

$$\begin{aligned} a &\equiv x_1(\text{mod } p) \\ 2a &\equiv x_2(\text{mod } p) \\ &\vdots \quad\quad \vdots \\ (p-1)a &\equiv x_{p-1}(\text{mod } p), \end{aligned}$$

onde $x_1,\ x_2,\ \ldots,\ x_{p-1}$ são os inteiros $1,\ 2,\ \ldots,\ p-1$, a menos da ordem.

Pelo Teorema 1.13 item $ii)$, vem:

$$\begin{aligned} a \cdot 2a \cdot \ldots \cdot (p-1)a &\equiv x_1 \cdot x_2 \cdot \ldots \cdot x_{p-1}(\text{mod } p) \\ &\equiv 1 \cdot 2 \cdot \ldots \cdot (p-1)(\text{mod } p), \end{aligned}$$

onde na última congruência o produto $x_1 \cdot x_2 \cdot \ldots \cdot x_{p-1}$ está posto ordenadamente. Logo,

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

Portanto, como $((p-1)!, p) = 1$, pelo corolário 1.5, advem que

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

■

Corolário 1.6. *Sejam $a,\ p \in \mathbb{Z}$, p-primo, a arbitrário. Então $a^p \equiv a(mod\ p)$.*

Demonstração. Se $p \nmid a$, do Teorema de Fermat temos que $a^{p-1} \equiv 1(\text{mod } p)$ e como $a \equiv a(\text{mod } p)$ pelo Teorema 1.13 item ii), vem:

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

Se $p|a$, então $p|aa^{p-1}$ o que implica $p|a^p$. Assim, $a = k_1p$ e $a^p = k_2p$. Multiplicando-se estas duas equações por -1 e 1, respectivamente, teremos $-a = -k_1p$ e $a^p = k_2p$. Somando-as, membro a membro, obtemos:

$$\begin{aligned} a^p - a = k_2p - k_1p &\Leftrightarrow a^p - a = (k_2 - k_1)p \\ &\Leftrightarrow p|(a^p - a) \\ &\Leftrightarrow a^p \equiv a(\text{mod } p). \end{aligned}$$

■

Definição 1.10. Se n é um inteiro positivo, a *função ϕ de Euler*, denotada por $\phi(n)$, é a definida como sendo o número de inteiros positivos menores do que ou iguais a n que são relativamente primos a n.

Definição 1.11. Um *Sistema Reduzido de Resíduos Módulo* m $(SRRM_{(m)})$ é um conjunto de $\phi(n)$ inteiros, $r_1,\ r_2,\ \ldots,\ r_{\phi(n)}$, tais que cada elemento do conjunto é relativamente primo com m, e se $i \neq j$, então $r_i \not\equiv r_j(\text{mod } m)$.

Exemplo 1.4. O conjunto $\{0,\ 1,\ 2,\ 4,\ 5\}$ é um $SCRM_{(6)}$, assim o conjunto $\{1,\ 5\}$ é um $SRRM_{(6)}$. Logo, note que de acordo com a definição 1.11, nosso exemplo serve para entendermos que se quisermos um $SRRM_{(m)}$, então é necessário apenas excluir os elementos do $SCRM_{(m)}$ que não são relativamente primos com m.

♦

Teorema 1.24. Sejam a e $m \in \mathbb{Z}_+^*$ tal que $(a, m) = 1$. Se o conjunto $\{r_1,\ r_2,\ \ldots,\ r_{\phi(m)}\}$ é um $SRRM_{(m)}$, então o conjunto $\{ar_1,\ ar_2,\ \ldots,\ ar_{\phi(m)}\}$, também, é um $SRRM_{(m)}$.

Demonstração. Usaremos o método de redução ao absurdo.

Como o conjunto $\{r_1,\ r_2,\ \ldots,\ r_{\phi(m)}\}$ é um $SRRM_{(m)}$, então pela definição 1.11, para $i \neq j$, temos que $r_i \not\equiv r_j(\text{mod } m),\ i, j \in \{1,\ 2,\ \ldots,\ \phi(m)\}$. Suponhamos por absurdo que, para $i \neq j$, existem ar_i e ar_j no conjunto $\{ar_1,\ ar_2,\ \ldots,\ ar_{\phi(m)}\}$ tais que $ar_i \equiv ar_j(\text{mod } m)$, $i, j \in \{1,\ 2,\ \ldots,\ \phi(m)\}$. Logo, como o $(a, m) = 1$, pelo Coroláro 1.5, então

$$\begin{aligned} ar_i \equiv ar_j(\text{mod } m) &\Rightarrow r_i \equiv r_j(\text{mod } m) \\ &\Rightarrow i = j, \ \text{ pois os } r_i,\ r_j \in SRRM_{(m)}. \end{aligned}$$

Mas, a tese $i = j$ é absurda, pois nossa hipótese é que $i \neq j$.

Portanto, o conjunto $\{ar_1,\ ar_2,\ \ldots,\ ar_{\phi(m)}\}$ é um $SRRM_{(m)}$. ■

Teorema 1.25. (Teorema de Euler): Sejam a e $m \in \mathbb{Z},\ 0 < m$, tal que $(a, m) = 1$. Então, é verdade que:

$$a^{\phi(m)} \equiv 1(\text{mod } m).$$

Demonstração. Seja $\mathcal{S} = \{r_1,\ r_2,\ \ldots,\ r_{\phi(m)}\}$ um $SRRM_{(m)}$. Então, se $(a, m) = 1$, pelo Teorema 1.24, também, o conjunto $\mathcal{A} = \{ar_1,\ ar_2,\ \ldots,\ ar_{\phi(m)}\}$ é um $SRRM_{(m)}$. Logo, para todo elemento $ar_i \in \mathcal{A}$ existe um único elemento $r_j \in \mathcal{S}$ tal que $ar_i \equiv r_j(\text{mod } m)$, onde $i,\ j \in \{1,\ 2,\ ,3,\ \ldots,\ \phi(m)\}$.

Portanto, pelo Teorema 1.13 item $ii)$, o produto de todos os elementos de $\mathcal{A}$ é congruente ao produto de todos os elementos de $\mathcal{S}$ módulo m, isto é,

$$ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\phi(m)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)}(\text{mod } m),$$

ou seja,

$$a^{\phi(m)} r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)}(\text{mod } m),$$

ou melhor,

$$a^{\phi(m)} \cdot \prod_{i=1}^{\phi(m)} r_i \equiv \prod_{i=1}^{\phi(m)} r_i(\text{mod } m), \tag{1.12}$$

Portanto, como o

$$\left(\prod_{i=1}^{\phi(m)} r_i, m \right) = 1,$$

então, pelo Corolário 1.5, podemos cancelar o produtório $\prod_{i=1}^{\phi(m)} r_i$ de ambos os membros da congruência 1.12 para advir

$$a^{\phi(m)} \equiv 1(\text{mod } m).$$

■

1.7 O TEOREMA DO RESTO CHINÊS

Em homenagem aos matemáticos chineses é um praxe entre os matemáticos em geral nomearem o próximo teorema como: o Teorema do Resto Chinês. Haja vista os chineses já o conhecerem desde a antiguidade.

Teorema 1.26. (Teorema do Resto Chinês): Se $(a_i, m_i) = 1$ e $(m_i, m_j) = 1$, para $i,\ j \in \{1,\ 2,\ \ldots,\ r\},\ i \neq j$, e $c_i \in \mathbb{Z}$, então o *sistema de congruências*

$$\begin{cases} a_1 x & \equiv & c_1(\text{mod } m_1) \\ a_2 x & \equiv & c_2(\text{mod } m_2) \\ a_3 x & \equiv & c_3(\text{mod } m_3) \\ \vdots & & \vdots \\ a_r x & \equiv & c_r(\text{mod } m_r) \end{cases}$$

tem uma única solução módulo m, onde $m = m_1 m_2 \cdots m_r$.

Demonstração. Como $(a_i, m_i) = 1$, então, pelo Teorema 1.19, há uma única solução à i-ésima congruência $a_i x \equiv c_i (\text{mod } m_i),\ i \in \{1,\ 2,\ \ldots,\ r\}$, a qual denotaremos por b_i. Seja $y_i = m/m_i$. Assim, como $(m_i, m_j) = 1$, então $(y_i, m_i) = 1$ para $i \neq j$. Logo, também, pelo Teorema 1.19, há uma única solução à i-ésima congruência $y_i x \equiv 1 (\text{mod } m_i)$, cuja denotaremos por $\overline{y}_i$. Dessa maneira, $y_i \overline{y}_i \equiv 1 (\text{mod } m_i),\ i \in \{1,\ 2,\ \ldots,\ r\}$.

Declaramos que o número x dado por

$$x = b_1 y_1 \overline{y}_1 + b_2 y_2 \overline{y}_2 + \cdots + b_r y_r \overline{y}_r \tag{1.13}$$

é a solução simultânea de nosso sistema de congruências. Com efeito, como

$$a_i x = a_i b_1 y_1 \overline{y}_1 + a_i b_2 y_2 \overline{y}_2 + \cdots + a_i b_i y_i \overline{y}_i + \cdots + a_i b_r y_r \overline{y}_r$$

e m_i divide todas as parcelas da soma $\displaystyle\sum_{j=1}^{r} a_i b_j y_j \overline{y}_j$, com excessão da parcela $a_i b_i y_i \overline{y}_i$, para $i \neq j$, pois em todas encontramos o termo $y_j = m_1 \cdot m_2 \cdots m_i \cdots m_r$, então:

$$\begin{aligned} a_i x &\equiv a_i b_i y_i \overline{y}_i (\text{mod } m_i) \\ &\equiv a_i b_i (\text{mod } m_i) \\ &\equiv c_i (\text{mod } m_i) \end{aligned}$$

onde, a penúltima congruência é válida porque $y_i \overline{y}_i \equiv 1 (\text{mod } m_i)$ e a última é válida porque b_i é solução da congruência $a_i x \equiv c_i (\text{mod } m_i)$.

Agora, devemos provar que a solução x da equação 1.13 é única módulo m.

Seja $\overline{x}$ outra solução para nosso sistema de congruências. Como, pelo Teorema 1.19, não outra solução incongrunete a x, acarreta que:

$$a_i \overline{x} \equiv c_i \equiv a_i x (\text{mod } m_i).$$

Mas, como $(a_i, m_i) = 1$, pelo Corolário 1.5, então

$$\begin{aligned} a_i \overline{x} \equiv a_i x (\text{mod } m_i) &\Rightarrow \overline{x} \equiv x (\text{mod } m_i) \\ &\Leftrightarrow m_i | (\overline{x} - x),\ i \in \{1,\ 2,\ \ldots,\ r\}. \end{aligned}$$

Assim, como $(m_i, m_j) = 1,\ \text{para } i \neq j$, então

$$[m_1,\ m_2,\ \ldots,\ m_r] = m_1 m_2 \cdots\ m_r = m.$$

e, pelo Teorema 1.15, $m | (\overline{x} - x)$, isto é,

$$\overline{x} \equiv x (\text{mod } m).$$

Logo, como $(a_i, m_i) = 1$ e $(m_i, m_j) = 1,$ para $i \neq j$tais que$i,\ j \in \{1,\ 2,\ \ldots,\ r\},$ e $c_i \in \mathbb{Z}$, então o sistema de congruências

$$\begin{cases} a_1 x & \equiv & c_1 (\text{mod } m_1) \\ a_2 x & \equiv & c_2 (\text{mod } m_2) \\ a_3 x & \equiv & c_3 (\text{mod } m_3) \\ \vdots & & \vdots \\ a_r x & \equiv & c_r (\text{mod } m_r) \end{cases}$$

tem uma única solução módulo $m,$ onde $m = m_1 m_2 \cdots m_r$. ■

2 FUNÇÕES ARITMÉTICAS

2.1 FUNÇÕES ARITMÉTICAS

Definição 2.1. Um função $f(n)$ é dita *função aritmética* se, e somente se, $f(n)$ está definida somente para todo $n \in \mathbb{Z}_+^*$.

Definição 2.2. Denotemos como $\tau(n)$ a função aritmética que nos *diz quantos são os divisores positivos de* n, e como $\sigma(n)$ a função aritmética que *soma todos os divisores positivos de* n. Portanto,

$$\tau(n) = \sum_{d|n} 1 \quad \text{e} \quad \sigma(n) = \sum_{d|n} d.$$

Teorema 2.1. Sejam $n,\ a_i$ e p_i-primo $\in \mathbb{Z}_+^*,\ i \in \{1,\ 2,\ \ldots,\ r\}$. Se a fatoração de n é dada por

$$n = p_1^{a_1} \cdot p_2^{a_2} \ldots p_r^{a_r},$$

então a função aritmética $\tau(n)$ é dada por

$$\tau(n) = \prod_{i=1}^{r} (a_i + 1).$$

Demonstração. Lembremos que:

$i)$ Sejam $a,\ b,\ d \in \mathbb{Z}_+^*$, tais que $(a, b) = 1$. Se $d|a \cdot b$, então existem d_1 e $d_2 \in \mathbb{Z}_+^*$, tais que $d_1|a,\ d_2|b$ e $d = d_1 \cdot d_2$. Reciprocamente, se existem d_1 e $d_2 \in \mathbb{Z}_+^*$ tais que $d_1|a$ e $d_2|b$, então $d|a \cdot b$, onde $d = d_1 \cdot d_2$.

$ii)$ *Princípio Fundamental da Contagem* (PFC): Se um evento é composto por n etapas sucessivas e independentes de tal maneira que

- m_1 é o número de possibilidades na 1ª etapa,
- m_2 é o número de possibilidades na 2ª etapa,
  . . . . . .
- m_n é o número de possibilidades na n-ésima etapa,

então o número de possibilidades de o evento ocorrer é dado por

$$m_1 \cdot m_2 \cdots m_n.$$

Seja $d \in \mathbb{Z}_+^*$ tal que $d|p_1^{a_1} \cdot p_2^{a_2} \ldots p_r^{a_r}$. Como $(p_1^{a_1},\ p_2^{a_2},\ \ldots,\ p_r^{a_r}) = 1$, então, pelo item $i)$ supracitado, existem $d_1,\ d_2,\ \ldots,\ d_r \in \mathbb{Z}_+^*$ tais que $d_1|p_1^{a_1},\ d_2|p_2^{a_2}, \ldots\ d_r|p_r^{a_r}$ e $d_1 \cdot d_2 \cdots d_r = d$, onde

$$\begin{array}{ccl} d_1 & \in & D_1 = \{p_1^{\alpha}\ ;\ 0 \leqslant \alpha \leqslant a_1\} \\ d_2 & \in & D_2 = \{p_2^{\alpha}\ ;\ 0 \leqslant \alpha \leqslant a_2\} \\ \cdots & \cdots & \cdots\cdots\cdots\cdots\cdots\cdots \\ d_r & \in & D_r = \{p_r^{\alpha}\ ;\ 0 \leqslant \alpha \leqslant a_r\}\,. \end{array}$$

Note que:

$$N(D_i) = a_i + 1,\ i \in \{1,\ 2,\ \ldots,\ r\},$$

isto é, dentro dos conjuntos $D_i \subset \mathbb{Z}_+^*$, existem $a_i + 1$ possibilidades para cada $d_i \in \mathbb{Z}_+^*$.

Portanto, como $d = d_1 \cdot d_2 \cdots d_r$ e para cada $d_i,\ i \in \{1,\ 2,\ \ldots,\ r\}$, existem $a_i + 1$ possibilidades, então, pelo PFC (item ii) supramencionado), para $d \in \mathbb{Z}_+^*$, existem $(a_1 + 1)(a_2 + 1)\cdots(a_r + 1)$ possibilidades de ocorrer que $d|n$, ou melhor,

$$\begin{aligned}\tau(n) &= (a_1 + 1)(a_2 + 1)\cdots(a_r + 1)\\ &= \prod_{i=1}^{r}(a_i + 1).\end{aligned}$$

■

Definição 2.3. Dizemos que uma função aritmética $f(n)$ (não-nula) é uma *função multiplicativa* se, e somente se, $(m, n) = 1$ e $f(m \cdot n) = f(m) \cdot f(n)$ para todo m e $n \in \mathbb{Z}_+^*$.

Definição 2.4. Dizemos que uma função aritmética $f(n)$ é *completamente multiplicativa* se, e somente se, $f(m \cdot n) = f(m) \cdot f(n)$ para todo m e $n \in \mathbb{Z}_+^*$.

Teorema 2.2. Se $f(n)$ é uma função multiplicativa, então a função

$$F(n) = \sum_{d|n} f(d)$$

é multiplicativa, também.

Demonstração. Pela definição de $F(n)$, vem:

$$F(m \cdot n) = \sum_{d|m\cdot n} f(d).$$

Como $(m, n) = 1$, pelo item i) enunciado na demonstração do Teorema 2.1, garantimos que se $d|m \cdot n$, então existem $d_1,\ d_2 \in \mathbb{Z}_+^*$ tais que $d_1|m,\ d_2|n$ e $d = d_1 \cdot d_2$.

Portanto,

$$F(m \cdot n) = \sum_{d|m\cdot n} f(d) = \sum_{\substack{d_1|m\\ d_2|n}} f(d_1 \cdot d_2).$$

Entretanto, como, por hipótese, f é multiplicativa, vem:

$$\begin{aligned}F(m \cdot n) &= \sum_{\substack{d_1|m\\ d_2|n}} f(d_1) \cdot f(d_2)\\ &= \sum_{d_1|m}\sum_{d_2|n} f(d_1) \cdot f(d_2)\\ &= \sum_{d_1|m} f(d_1) \cdot \sum_{d_2|n} f(d_2)\\ &= F(m) \cdot F(n).\end{aligned}$$

Logo, se a função $f(n)$ é multiplicativa, então a função

$$F(n) = \sum_{d|n} f(d).$$

é multiplicativa, também. ■

Corolário 2.1. *As funções $\tau(n)$ e $\sigma(n)$ são multiplicativas.*

Demonstração. Como

$$\tau(n) = \sum_{d|n} 1 \qquad \text{e} \qquad \sigma(n) = \sum_{d|n} d,$$

então $f_\tau(d) = 1$ e $f_\sigma(d) = d$.

Portanto, como $f_\tau(d)$ e $f_\sigma(d)$ são multiplicativas, então pelo Teorema 2.2 as funções $\tau(n)$ e $\sigma(n)$ são multiplicativas. ■

Teorema 2.3. Sejam a e $p \in \mathbb{Z}_+^*,\ p$-primo. Então, é verdade que:

$$\sigma(p^a) = \frac{p^{a+1} - 1}{p - 1} \qquad \text{e} \qquad \tau(p^a) = a + 1.$$

Demonstração. Lembremos que:

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1}, \text{ para } x \in \mathbb{Z}_+^* - \{1\} \tag{2.1}$$

É sabido, pela demonstração do Teorema 2.1, que $\tau(p^a) = a + 1$. Como, pela Definição 2.2, sabemos que $\sigma(p^a) = 1 + p + p^2 + \cdots + p^a$, então da Equação 2.1 garante que

$$\sigma(p^a) = \frac{p^{a+1} - 1}{p - 1}.$$

■

Teorema 2.4. Seja $n \in \mathbb{Z} - \{-1,\ 0,\ 1\}$, tal que $n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_r^{a_r}$. Então, é verdade que

$$\sigma(n) = \prod_{i=1}^{r} \frac{{p_i}^{a_i+1} - 1}{p_i - 1} \qquad \text{e} \qquad \tau(n) = \prod_{i=1}^{r} (a_i + 1).$$

Demonstração. Como as funções aritméticas $\tau(n)$ e $\sigma(n)$ são multiplicativas, então, pelo Teorema 2.3, são válidas as seguintes manipulações algébricas abaixo:

$$\begin{aligned} \tau(n) &= \tau(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}) \\ &= \tau(p_1^{a_1})\tau(p_2^{a_2}) \cdots \tau(p_r^{a_r}) \\ &= (a_1 + 1)(a_2 + 1)(a_r + 1) \\ &= \prod_{i=1}^{r} (a_i + 1) \end{aligned}$$

e

$$\begin{aligned}\sigma(n) &= \sigma(p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}) \\ &= \sigma(p_1^{a_1})\sigma(p_2^{a_2})\cdots\sigma(p_r^{a_r}) \\ &= \frac{p_1^{a_1+1}-1}{p_1-1}\cdot\frac{p_2^{a_2+1}-1}{p_2-1}\cdots\frac{p_r^{a_r+1}-1}{p_r-1} \\ &= \prod_{i=1}^{r}\frac{p_i^{a_i+1}-1}{p_i-1}.\end{aligned}$$

2.2 A FUNÇÃO ϕ DE EULER

Teorema 2.5. Sejam a e $p \in \mathbb{Z}_+^*,\ p$-primo. Então, é verdade que

$$\phi(p^a) = p^a - p^{a-1}.$$

Demonstração. Recordemos que denotamos $\phi(n)$ (difinição 1.10) como a quantidade de números inteiros positivos $b \leqslant n$ tais que o $(b,n) = 1$. Porém, os únicos inteiros positivos não-primos com e não-superiores a p^a são os múltiplos de p, isto é,

$$1\cdot p,\ 2\cdot p,\ \ldots,\ p^{a-1}\cdot p. \tag{2.2}$$

Portanto, como $p = p^{a-1}\cdot p$, então, em quantidade, os múltiplos de p não-superiores a p^a são p^{a-1} (observe a sequência 2.2 que são os múltiplos de p não-superiores a p^a).

Logo, a quantidade de números inteiros positivos $b \leqslant p^a$ tais que o $(b,p^a) = 1$ é dada por

$$\phi(p^a) = p^a - p^{a-1}.$$

■

Teorema 2.6. A função ϕ de Euler é multiplicativa, isto é,

$$\phi(m\cdot n) = \phi(m)\cdot\phi(n),$$

$\forall m,\ n \in \mathbb{Z}_+^*$, tais que $(m,n) = 1$.

Demonstração. Inicialmente, lembremos do Lema de Euclides enunciado no item $i)$ abaixo.

$i)$ Sejam $a,\ b,\ x \in \mathbb{Z}$. Se existe $(a, ax+b)$, então existe (a,b) e

$$(a,b) = (a, ax+b).$$

Organizemos os números de 1 até $mn\ (= nm)$ como os elementos de uma matriz de ordem $m\times n$, isto é,

$$\begin{pmatrix} 1 & m+1 & 2m+1 & \ldots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \ldots & (n-1)m+2 \\ 3 & m+3 & 2m+3 & \ldots & (n-1)m+3 \\ \vdots & \vdots & \vdots & & \vdots \\ m & 2m & 3m & \ldots & nm \end{pmatrix}.$$

Note que, para $r \in \{1,\ 2,\ 3,\ \ldots,\ m\}$, na r-ésima linha de elementos $r,\ m+r,\ 2m+r,\ \ldots,\ (n-1)m+r$, se $(m,r) = d > 1$, então não existirá elemento $km+r$, $k \in \{0,\ 1,\ 2, \ldots,\ n-1\}$, na r-ésima linha, tal que $(mn, km+r) = 1$, pois todos os elementos da r-ésima linha são divisíveis por d, o qual é o máximo divisor comum de m e r. Com isto, em nossa matriz $m \times n$, garantimos que para encontrar elementos primos com o produto $m \cdot n$ devemos avaliar, inicialmente na r-ésima linha, se $(m,r) = 1$.

Por outro lado, pelo Lema de Euclides supradescrito, $(m,r) = (m, km+r)$, isto é, se $(m,r) = 1$, então existe $\phi(m)$ linhas, em nossa matriz $m \times n$, às quais todos os elementos são primos com m. Mas, em cada uma destas $\phi(m)$ linhas, quantos elementos são primos com n? Para responder esta pergunta vamos meditar atentamente sobre as características da r-ésima linha supracitada.

Como $(m,n) = 1$ e $\{0,\ 1,\ 2,\ \ldots,\ n-1\}$ é um $SCRM_{(n)}$, então, pelo Teorema 1.16, a r-ésima linha, também, é um $SCRM_{(n)}$. Todavia, como na r-ésima linha podem existir números maiores do que n, então representaremos tais números por seu represetante do conjunto $\{0,\ 1,\ 2,\ \ldots,\ n-1\}$ (ver a Observação **??**) para, com a definição de $\phi(n)$ em mente, garantirmos a existência de $\phi(n)$ números relativamente primos com n em cada uma das $\phi(m)$ linhas (isto responde nossa pergunta supramencionada, no parágrafo anterior desta demonstração).

Portanto, como em cada uma das $\phi(m)$ linhas existem $\phi(n)$ elementos relativamente primos com m e n simultaneamente, então, em nossa matriz de ordem $m \times n$, existem $\phi(m) \cdot \phi(n)$ elementos relativamente primos com o produto $m \cdot n$, ou melhor,

$$\phi(m \cdot n) = \phi(m) \cdot \phi(n).$$

Logo, a função ϕ de Euler é multiplicativa. ■

Teorema 2.7. Seja $n \in \mathbb{Z} - \{-1, 0, 1\}$. Então, para $n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_r^{a_r}$, é válido o seguite resultado:

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

Demonstração. Do Teorema 2.5, vem:

$$\phi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i - 1} = p_i^{a_i}\left(1 - \frac{1}{p_i}\right).$$

Por outro lado, como, pelo Teorema 2.6, a função ϕ de Euler é uma função multiplicativa, então:

$$\begin{aligned}
\phi(n) = \phi(p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_r^{a_r}) &= \phi(p_1^{a_1})\phi(p_2^{a_2})\phi(p_3^{a_3})\cdots\phi(p_r^{a_r}) \\
&= p_1^{a_1}\left(1 - \frac{1}{p_1}\right) p_2^{a_2}\left(1 - \frac{1}{p_2}\right)\cdots p_r^{a_r}\left(1 - \frac{1}{p_r}\right) \\
&= p_1^{a_1} p_2^{a_2}\cdots p_r^{a_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_r}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_r}\right).
\end{aligned}$$

Logo, é válido que para $n = p_1^{a_1}p_2^{a_2}p_3^{a_3}\cdots p_r^{a_r},\ n \in \mathbb{Z} - \{-1, 0, 1\}$,

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

■

Teorema 2.8. Seja $n \in \mathbb{Z}$. Então,

$$\sum_{d|n} \phi(d) = n.$$

Demonstração. Lembremos que

$i)$ Sejam d e $n \in \mathbb{Z},\ d \neq 0$. Se $d|n$, então $(n/d)|n$;

$ii)$ Sejam $a,\ b$ e $c \in \mathbb{Z}$. Se $(m, n) = c$, então $\left(\frac{m}{c}, \frac{n}{c}\right) = 1$.

Consideremos o conjunto $\{1,\ 2,\ 3, \ldots,\ n\}$ e o dividamos em subconjuntos A_d, um para cada divisor d de n. No subconjunto A_d deixaremos todos os membros m, onde $m \in \{1,\ 2,\ \cdots,\ n\}$, tais que $(m, n) = d$. Pelo item $ii)$ acima, como $m/d \leqslant n/d$, então m está em A_d se $(m/d, n/d) = 1$. Assim, em A_d temos exatamente $\phi(n/d)$ membros. Como cada membro de $\{1,\ 2,\ 3, \ldots,\ n\}$ se acha apenas em um dos subconjuntos A_d e, pelo item $i)$ acima, para cada divisor d de n, também, n/d é um divisor de n, então:

$$\sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d) = n.$$

■

2.3 A FUNÇÃO μ DE MÖBIUS

Definição 2.5. A função μ de Möbius é definida como

$$\mu(n) = \begin{cases} 1, & \text{se} \quad n = 1 \\ (-1)^r, & \text{se} \quad n = p_1^{a_1}p_2^{a_2}p_3^{a_3}\cdots p_r^{a_r} \quad \text{e} \quad a_1 = a_2 = a_3 = \ldots = a_r = 1 \\ 0, & \text{se} \quad n = p_1^{a_1}p_2^{a_2}p_3^{a_3}\cdots p_r^{a_r} \quad \text{e} \quad \exists a_i,\ i \in \{1,\ 2,\ 3,\ \ldots,\ r\} \text{ tal que } a_i > 1. \end{cases}$$

Observação 1. Em outras palavras, a Definição 2.5 afirma que se $\mu(n) = 0$, então n é divisível pelo quadrado de algum p-primo.

Teorema 2.9. A função μ de Möbius é multiplicativa.

Demonstração. Sejam m e $n \in \mathbb{Z}_+^*$ tais que $(m, n) = 1$.

Primeiro, se $n = 1$ ou $m = 1$, então é óbvio que $\mu(m \cdot n) = \mu(m) \cdot \mu(n)$.

Segundo, suponhamos que existe p-primo tal que $p^2|(m \cdot n)$, então

$$p^2|m \ \text{ ou } \ p^2|n,$$

pois $(m, n) = 1$. Logo,

$i)$ Se $p^2|m$, então $\mu(m) = 0$ e $\mu(m \cdot n) = 0$ e, portanto, $\mu(m) \cdot \mu(n) = 0$, ou seja,

$$\mu(m \cdot n) = \mu(m) \cdot \mu(n);$$

$ii)$ Se $p^2|n$, então $\mu(n) = 0$ e $\mu(m \cdot n) = 0$ e, assim, $\mu(m) \cdot \mu(n) = 0$, isto é,

$$\mu(m \cdot n) = \mu(m) \cdot \mu(n).$$

E terceiro, se não existir p-primo tal que $p^2|m$ ou $p^2|n$, então para m e $n \in \mathbb{Z}_+^* - \{1\}$, o *Teorema Fundamental da Aritmética* (TFA), nos garante que:

$$m = p_1 \cdot p_2 \cdots p_r \quad \text{e} \quad n = q_1 \cdot q_2 \cdots q_s$$

e, portanto, $m \cdot n = \underbrace{p_1 \cdot p_2 \cdots p_r \cdot q_1 \cdot q_2 \cdots q_s}_{(r+s) \text{ fatores primos}}$.

Logo,

$$\mu(m \cdot n) = (-1)^{r+s} = (-1)^r \cdot (-1)^s = \mu(m) \cdot \mu(n).$$

Portanto, a função μ de Möbius é multiplicativa. ■

Teorema 2.10. Seja $n \in \mathbb{Z}_+^*$. Então, é verdade que

$$F(n) = \sum_{d|n} \mu(d) = \begin{cases} 1, & \text{se} \quad n = 1 \\ 0, & \text{se} \quad n > 1. \end{cases}$$

Demonstração. Note que, pela denfinição de $\mu(n)$ (Definição 2.5), se $n = 1$, então:

$$F(1) = \sum_{d|1} \mu(d) \overset{d|1 \Rightarrow d=1}{=} \sum_{1|1} \mu(1) = \mu(1) = 1.$$

Entretanto, na soma

$$\sum_{d|n} \mu(d)$$

os únicos termos que não são nulos resultam de $d = 1$, ou dos divisores que são produto de primos diferentes, ou seja,

$$\begin{aligned} F(n) = \sum_{d|n} \mu(d) &= 1 + \mu(p_1) + \cdots + \mu(p_r) + \mu(p_1p_2) + \mu(p_1p_3) + \\ &\quad + \cdots + \mu(p_1p_r) + \cdots + \mu(p_1p_2 + \cdots + p_r) \\ &= 1 + \binom{r}{1}(-1) + \binom{r}{2}(-1)^2 + \cdots + \binom{r}{r}(-1)^r \\ &= (1-1)^r = 0 \end{aligned}$$

Logo, como para $n = 1$ se tem $F(n) = 1$, e para todo $n > 1$ se tem $F(n) = 0$, então:

$$F(n) = \sum_{d|n} \mu(d) = \begin{cases} 1, & \text{se} \quad n = 1 \\ 0, & \text{se} \quad n > 1. \end{cases}$$

■

2.4 A FUNÇÃO MAIOR INTEIRO

Definimos, abaixo, a função *"maior inteiro"*. Esta é ma importante função m Teoria dos Número que introduzimos aqui, em bora não seja, pela nossa definição, uma função aritmética.

Definição 2.6. A função *"maior inteiro"* é a que associa a cada número real x o maior inteiro menor do que ou igual a x, ao qual denotamos por $\lfloor x \rfloor$.

Exemplo 2.1. $\lfloor 3 \rfloor = 3, \lfloor 0,5 \rfloor = 0, \lfloor -4,9, \rfloor = -5, \lfloor 2,2 \rfloor = 2, \lfloor -0,9 \rfloor = -1.$

Teorema 2.11. Para um número real x, temos:

1. $\lfloor x + n \rfloor = \lfloor x \rfloor + n, \ \forall n \in \mathbb{Z}$;
2. $\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1, \ x - 1 < \lfloor x \rfloor \leqslant x, \ 0 \leqslant x - \lfloor x \rfloor < 1$;
3. $x \notin \mathbb{Z} \Rightarrow \lfloor -x \rfloor = -\lfloor x \rfloor - 1$;
4. $\lfloor x \rfloor + \lfloor y \rfloor \leqslant \lfloor x + y \rfloor \leqslant \lfloor x \rfloor + \lfloor y \rfloor + 1$;
5. $\lfloor x \rfloor + \lfloor -x \rfloor = \begin{cases} 0, & \text{se} \quad x \in \mathbb{Z} \\ -1, & \text{se} \quad x \notin \mathbb{Z}; \end{cases}$
6. $\left\lfloor \dfrac{\lfloor x \rfloor}{k} \right\rfloor = \left\lfloor \dfrac{x}{k} \right\rfloor, \ k \in \mathbb{Z}_+^*$;
7. $\lfloor 2x \rfloor - 2\lfloor x \rfloor = \begin{cases} 0, & \text{se} \quad \lfloor 2x \rfloor \quad \text{é par} \\ 1, & \text{se} \quad \lfloor 2x \rfloor \quad \text{é ímpar}; \end{cases}$
8. $n \in \mathbb{Z}_+$ e $a \in \mathbb{Z}^* \Rightarrow \left\lfloor \dfrac{n}{a} \right\rfloor = \sum_{a|b} 1, \ b \in \{1, \ 2, \ \ldots, \ n\}$;
9. $\left\lfloor \dfrac{\left\lfloor \frac{a}{b} \right\rfloor}{c} \right\rfloor = \left\lfloor \dfrac{a}{bc} \right\rfloor, \forall a \in \mathbb{Z}_+,$ e $\forall b$ e $c \in \mathbb{Z}_+^*$.

Demonstração. As afirmações $(1), (2)$ e (3) são consequências imediatas da definição de $\lfloor x \rfloor$. Sejam $x = n + u$ e $y = m + v$, onde n e $m \in \mathbb{Z}$ e $0 \leqslant u < 1, 0 \leqslant v < 1$, (usaremos estes dados

nas demonstrações dos itens de (4) a (8)). Logo,

(4)

$$\begin{aligned}\lfloor x\rfloor+\lfloor y\rfloor &= n+m\\ &= \lfloor n+m\rfloor\\ &\leqslant \lfloor n+u+m+v\rfloor\\ &= \lfloor x+y\rfloor\\ &= n+m+\lfloor u+v\rfloor\\ &\leqslant n+m+1\\ &= \lfloor x\rfloor+\lfloor y\rfloor+1.\end{aligned}$$

(5)

$$\begin{aligned}\lfloor x\rfloor+\lfloor -x\rfloor &= n+\lfloor -n-u\rfloor\\ &= n+\lfloor -n-1+1-u\rfloor\\ &\overset{(1)}{=} n-n-1+\lfloor 1-u\rfloor\\ &= \begin{cases} 0, & \text{se} \quad u=0\\ -1, & \text{se} \quad 0<u<1.\end{cases}\end{aligned}$$

(6) É sabido que, pelo Algoritmo da Divisão, existem únicos k e $r\in\mathbb{Z}$ tais que $n=kq+r$, $0\leqslant r\leqslant k-1$. Portanto,

$$\left\lfloor\frac{x}{k}\right\rfloor=\left\lfloor\frac{kq+r+u}{k}\right\rfloor=\left\lfloor q+\frac{r+u}{k}\right\rfloor=q, \tag{2.3}$$

pois, $0\leqslant r+u<k$, haja vista $0\leqslant u<1$ e $0\leqslant r<k-1$. Todavia,

$$\left\lfloor\frac{\lfloor x\rfloor}{k}\right\rfloor=\left\lfloor\frac{n}{k}\right\rfloor=\left\lfloor\frac{kq+r}{k}\right\rfloor=\left\lfloor q+\frac{r}{k}\right\rfloor=q. \tag{2.4}$$

Logo, das equações (2.3) e (2.4)

$$\left\lfloor\frac{\lfloor x\rfloor}{k}\right\rfloor=\left\lfloor\frac{x}{k}\right\rfloor.$$

(7) Como $0\leqslant u<1,$ então $\left(0\leqslant u\leqslant\frac{1}{2}\right)\bigcup\left(\frac{1}{2}\leqslant u<1\right)$.

$i)$ Se $0\leqslant u\leqslant\frac{1}{2}$, então $2u<1$. Daí,

$$\begin{aligned}\lfloor 2x\rfloor &= \lfloor 2n+2u\rfloor\\ &= 2n\\ &\Leftrightarrow \lfloor 2x\rfloor \text{ é par.}\end{aligned}$$

Logo,

$$\begin{aligned}\lfloor 2x\rfloor-2\lfloor x\rfloor &= 2n-2n\\ &= 0.\end{aligned}$$

$ii)$ Se $\frac{1}{2} \leqslant u \leqslant 1$, então $1 \leqslant 2u < 2$. Daí,

$$\begin{aligned} \lfloor 2x \rfloor &= \lfloor 2n + 2u \rfloor \\ &= 2n + 1 \\ &\Leftrightarrow \lfloor 2x \rfloor \text{ é ímpar.} \end{aligned}$$

Assim,

$$\begin{aligned} \lfloor 2x \rfloor - 2\lfloor x \rfloor &= 2n + 1 - 2n \\ &= 1. \end{aligned}$$

Portanto,

$$\lfloor 2x \rfloor - 2\lfloor x \rfloor = \begin{cases} 0, & \text{se } \lfloor 2x \rfloor \text{ é par} \\ 1, & \text{se } \lfloor 2x \rfloor \text{ é ímpar.} \end{cases}$$

(8) O enunciado desse item afirma que: "se n é um inteiro positivo, então $\left\lfloor \frac{n}{a} \right\rfloor$ é o número (a quantidade) de inteiros do conjunto $\{1,\ 2,\ \ldots,\ n\}$ que são divisíveis por $a \in \mathbb{Z}^*$".

Seja $q \in \mathbb{Z}$. Lembremos que o quociente q entre n e a é a quantidade de vezes inteiras que a cabe dentro de n. Logo, os múltiplos de a entre 1 e n são $1 \cdot a,\ 2 \cdot a,\ 3 \cdot a\ \ldots,\ q \cdot a$, isto é, existe q números entre 1 e n divisíveis por a.

Por outro lado, pelo Algoritmo da Divisão, temos:

$$n \ = \ a \cdot q + r, \quad 0 \leqslant r \leqslant a \tag{2.5}$$

Dividamos a sentença 2.5 por a; logo,

$$\frac{n}{a} \ = \ q + \frac{r}{a}, \quad 0 \leqslant \frac{r}{a} \leqslant 1. \tag{2.6}$$

Apliquemos a função maior inteiro na equação 2.6; logo,

$$\left\lfloor \frac{n}{a} \right\rfloor = \left\lfloor q + \frac{r}{a} \right\rfloor \overset{(1)}{=} \lfloor q \rfloor + \left\lfloor \frac{r}{a} \right\rfloor \overset{(2.6)}{=} q + 0 = q.$$

Todavia, pela sentença 2.5, $\left\lfloor \frac{n}{a} \right\rfloor = q$ significa que os seguintes números que são divisíveis por a

$$1 \cdot a,\ 2 \cdot a,\ 3 \cdot a\ \ldots,\ \left\lfloor \frac{n}{a} \right\rfloor \cdot a, \tag{2.7}$$

estão entre 1 e n, ou melhor, os números da sequência 2.7 são divisíveis por a e pertencem ao conjunto $\{1,\ 2,\ \ldots,\ n\}$.

Portanto, se n é um inteiro positivo, então $\left\lfloor \frac{n}{a} \right\rfloor$ é a quantidade de números inteiros do conjunto $\{1,\ 2,\ \ldots,\ n\}$ que são divisíveis pelo inteiro a $(a \neq 0)$, isto é,

$$n \in \mathbb{Z}_+^* \Rightarrow \left\lfloor \frac{n}{a} \right\rfloor = \sum_{a|b} 1,\ a \in \mathbb{Z}^* \text{ e } b \in \{1,\ 2,\ \ldots,\ n\}.$$

Para ilustrar esse fato, damos o seguinte exemplo:

Exemplo 2.2. Sejam $n = 20$ e $a = 5$. Logo, $b \in \{1,\ 2,\ 3,\ \ldots,\ 20\}$ e, portanto,

$$\left\lfloor \frac{20}{5} \right\rfloor = \sum_{5|b} 1 = 1 + 1 + 1 + 1 = 4,$$

pois no conjunto $\{1,\ 2,\ 3,\ \ldots,\ 20\}$ são divisíveis por 5 os númros $5,\ 10,\ 15$ e 20, apenas. Além disso,

$$20 = \left\lfloor \frac{20}{5} \right\rfloor 5 + 0.$$

(9) Sejam $a,\ q_1$ e $q_2 \in \mathbb{Z}_+,$ e b e $c \in \mathbb{Z}_+^*$ tais que

$$q_1 = \left\lfloor \frac{a}{b} \right\rfloor \text{ e } q_2 = \left\lfloor \frac{\left\lfloor \frac{a}{b} \right\rfloor}{c} \right\rfloor,$$

onde pelo item (8) q_1 e q_2 são os quocintes de suas respectivas divisões.

Logo, pelo Algoritmo da Divisão,

$$a = b \cdot q_1 + r_1, \quad 0 \leqslant r_1 \leqslant b - 1 \tag{2.8}$$

$$\left\lfloor \frac{a}{b} \right\rfloor = c \cdot q_2 + r_2, \quad 0 \leqslant r_2 \leqslant c - 1. \tag{2.9}$$

Como $q_1 = \left\lfloor \frac{a}{b} \right\rfloor$, então substituindo a equação 2.9 na equação 2.8, obtemos:

$$a = b(cq_2 + r_2) + r_1 \Leftrightarrow a = bcq_2 + br_2 + r_1. \tag{2.10}$$

Agora, para provarmos que na equação $2.10,\ q_2$ é o quociente da divisão euclidiana de a por bc, ou seja, $q_2 = \left\lfloor \frac{a}{bc} \right\rfloor$, multipliquemos a inequação 2.9 por b, para obtermos:

$$0 \leqslant br_2 \leqslant b(c - 1). \tag{2.11}$$

Somemos a inequação 2.11 com a inequação 2.8, para obtermos:

$$0 \leqslant br_2 + r_1 \leqslant b(c - 1) + b - 1 \Leftrightarrow 0 \leqslant br_2 + r_1 \leqslant bc - b + b - 1.$$

E, portanto:

$$0 \leqslant br_2 + r_1 \leqslant bc - 1 \tag{2.12}$$

Logo, emparelhando a equação 2.10 com a inequação 2.12, isto é,

$$a = (bc)q_2 + (br_2 + r_1), \quad 0 \leqslant br_2 + r_1 \leqslant bc - 1$$

deduzimoms que q_2 é o quociente da divisão euclidiana de a por bc, ou melhor,

$$\left\lfloor \frac{\left\lfloor \frac{a}{b} \right\rfloor}{c} \right\rfloor = \left\lfloor \frac{a}{bc} \right\rfloor,$$

$\forall a \in \mathbb{Z}_+,$ e $\forall b$ e $c \in \mathbb{Z}_+^*$. ■

Observação 2. Conhecida a função *"maior inteiro",* podemos enunciar o Teorema 2.10 como

$$F(n) = \sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor, \ \ n \in \mathbb{Z}_+^*.$$

Sejam x e $p \in \mathbb{N}$, p-primo. Denotamos por $E_p(x)$ o expoente da maior potência de p que divide x. Em particular, a notação $E_p(n!)$ simbolia o expoente da maior potência de p que divide $n!$.

Teorema 2.12. (Teorema de Legendre) Sejam n, $p \in \mathbb{N}$, p-primo. Então, o expoente da maior potência de p que divide $n!$ é dado por:

$$E_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \cdots \tag{2.13}$$

Demonstração. Inicialmente, mostraremos que a série 2.13 é finita.

Seja $\alpha \in \mathbb{N}$ tal que $\left\lfloor \frac{n}{p^\alpha} \right\rfloor = 0$. Como, pela definição 2.6, a função maior intero é dada por

$$\begin{array}{rccc} \text{f}: & \mathbb{R} & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & \lfloor x \rfloor = y, \end{array}$$

onde $\lfloor x \rfloor = y \Leftrightarrow y \leq x < y + 1$, então

$$\left\lfloor \frac{n}{p^\alpha} \right\rfloor = 0 \Rightarrow 0 = \frac{n}{p^\alpha} < 1 \tag{2.14}$$

Na dupla inequação 2.14, o fato $\dfrac{n}{p^\alpha} < 1$ é bastante relevante, pois dele é possível extrair uma relação de ordem que envolve α diretamente, isto é,

$$\begin{aligned} \frac{n}{p^\alpha} \Leftrightarrow n < p^\alpha &\Leftrightarrow \log n < \log p^\alpha \\ &\Leftrightarrow \log n < \alpha \log p. \\ &\Leftrightarrow \alpha > \frac{\log n}{\log p} \end{aligned}$$

Seja $\alpha_1 = \min \left\{ \alpha \in \mathbb{N}^* \ ; \ \alpha > \dfrac{\log n}{\log p} \right\}$ e façamos $\alpha_1 = s(k) = k + 1, \ \ k \in \mathbb{N}^*$. Com isto, garantimos que

$$p^k \leq n \Leftrightarrow k = \left\lfloor \frac{\log n}{\log p} \right\rfloor \Leftrightarrow k \leq \frac{\log n}{\log p} < k + 1 \tag{2.15}$$

Portanto, do fato que $\left\lfloor \dfrac{n}{p^{\alpha_1}} \right\rfloor = 0$ e pela expressão 2.15,

$$0 < \left\lfloor \frac{n}{p^k} \right\rfloor \leq \left\lfloor \frac{n}{p^i} \right\rfloor \leq \left\lfloor \frac{n}{p^1} \right\rfloor, \ \ i \in \{1, \ 2, \ldots, \ k\},$$

ou melhor,

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^k} \right\rfloor, \tag{2.16}$$

onde $k = \left\lfloor \dfrac{\log n}{\log p} \right\rfloor$, haja vista apartir do $s(k)$ ocorrer $\left\lfloor \dfrac{n}{p^{\alpha}} \right\rfloor = 0$. Logo, pela definição pela equação 2.16, a série 2.13 é finita. Agora, como pelo item (8) do Teorema 2.8,

$$\left\lfloor \frac{n}{p^i} \right\rfloor = \sum_{p^i|\delta} 1, \ \ \delta \in \{1,\ 2, \ldots,\ n\} \tag{2.17}$$

isto é, $\left\lfloor \dfrac{n}{p^i} \right\rfloor$ soma o número (faz a contagem) de múltiplos de p^i entre 1 e n, os quais são

$$1 \cdot p^i,\ 2 \cdot p^i, \ldots, \left\lfloor \frac{n}{p^i} \right\rfloor \cdot p^i,$$

então, em outras palavras, de acordo com equação 2.17:

- $\sum_{p|\delta} 1$ faz a contagem $($entre 1 e $n)$ de um fator p em cada um dos múltiplos de p^{β_1}, $\beta_1 \in \{1,\ 2,\ \ldots,\ k\};$ mas, nessa contagem, não são contados $(\beta_2 - 1)$ fatores de p nas potências de $p^{\beta_2},\ \beta_2 \in \{2,\ 3, \ldots,\ k\};$
- $\sum_{p|\delta} 1 + \sum_{p^2|\delta} 1$ faz a contagem anterior e a contagem de mais um fator p em cada um dos múltiplos de $p^{\beta_2};$ mas, nessa contagem, não são contados $(\beta_3 - 2)$ fatores de p nas potências de $p^{\beta_3},\ \beta_3 \in \{3,\ 4, \ldots,\ k\};$
- $\sum_{p|\delta} 1 + \sum_{p^2|\delta} 1 + \sum_{p^3|\delta} 1$ faz a contagem anterior e a contagem de mais um fator p em cada um dos múltiplos de $p^{\beta_3};$ mas, nessa contagem, não são contados $(\beta_4 - 3)$ fatores de$p$ nas potências de $p^{\beta_4},\ \beta_4 \in \{4,\ 5, \ldots,\ k\};$

$\vdots \ + \ \vdots \ + \ \vdots \ + \ \vdots$ ....

- $\sum_{p|\delta} 1 + \sum_{p^2|\delta} 1 + \sum_{p^3|\delta} 1 + \cdots + \sum_{p^k|\delta} 1$ faz a contagem anterior e a contagem do último fator p no único múltiplo de $p^{\beta_k},\ \beta_k \in \{k\}$. Ora, de acordo com a expressão $2.15,$ como $p^{s(k)}$ não está na expansão de $n!$, então a contagem $\sum_{i=1}^{k} \left(\sum_{p^i|\delta} 1 \right)$ considera todos os fatores p presentes em todos os múltiplos de $p^i,\ i \in \{1,\ 2,\ \ldots,\ k\}$, que estão na expansão de $n!$.

Portanto

$$\sum_{i=1}^{k} \left(\sum_{p^i|\delta} 1 \right)$$

representa o maior expoente de p tal que

$$p^{\left[\sum_{i=1}^{k} \left(\sum_{p^i|\delta} \right) \right]} | n!,$$

isto é,

$$\begin{aligned} E_p(n!) &= \sum_{i=1}^{k}\left(\sum_{p^i|\delta} 1\right) \\ &= \sum_{p|\delta} 1 + \sum_{p^2|\delta} 1 + \sum_{p^3|\delta} 1 + \cdots + \sum_{p^k|\delta} 1 \\ &\overset{(2.17)}{=} \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^k} \right\rfloor \\ &\overset{(2.16)}{=} \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots . \end{aligned}$$

■

Teorema 2.13. Sejam $n,\ n_1,\ n_2, \ldots,\ n_s \in \mathbb{N}$ tais que

$$n = n_1 + n_2 + \cdots + n_s.$$

Então, é verdade que

$$\frac{n!}{n_1!n_2!\cdots n_s!}$$

é um número inteiro positivo.

Demonstração. Seja $m \in \mathbb{Z}_+^*$. Como $n = n_1 + n_2 + \cdots + n_s$, então

$$\frac{n}{m} = \frac{n_1}{m} + \frac{n_2}{m} + \cdots + \frac{n_s}{m}. \tag{2.18}$$

Apliquemos o item (4) do Teorema 2.11 na equação 2.18 para gerarmos a seguinte desigualdade

$$\left\lfloor \frac{n}{m} \right\rfloor \geqslant \left\lfloor \frac{n_1}{m} \right\rfloor + \left\lfloor \frac{n_2}{m} \right\rfloor + \cdots + \left\lfloor \frac{n_s}{m} \right\rfloor . \tag{2.19}$$

Seja p-primo um fator de $n!$. Substituamos o m da desigualdade 2.19 por $p,\ p^2,\ p^3 \ldots,$ sucessivamente. Isto é,

$$\begin{array}{ccccccccc} \left\lfloor \frac{n}{p} \right\rfloor & \geqslant & \left\lfloor \frac{n_1}{p} \right\rfloor & + & \left\lfloor \frac{n_2}{p} \right\rfloor & + & \cdots & + & \left\lfloor \frac{n_s}{p} \right\rfloor \\ \left\lfloor \frac{n}{p^2} \right\rfloor & \geqslant & \left\lfloor \frac{n_1}{p^2} \right\rfloor & + & \left\lfloor \frac{n_2}{p^2} \right\rfloor & + & \cdots & + & \left\lfloor \frac{n_s}{p^2} \right\rfloor \\ \left\lfloor \frac{n}{p^3} \right\rfloor & \geqslant & \left\lfloor \frac{n_1}{p^3} \right\rfloor & + & \left\lfloor \frac{n_2}{p^3} \right\rfloor & + & \cdots & + & \left\lfloor \frac{n_s}{p^3} \right\rfloor \\ \vdots & & \vdots & & \vdots & & & & \vdots \end{array}$$

Somando-se, membro a membro, todas as desigualdade obtidas acima, pelo Teorema **??** (o Teorema de Legendre), obtemos:

$$E_p(n!) \;\geqslant\; E_p(n_1!) \;+\; E_p(n_2!) \;+\; \cdots \;+\; E_p(n_s!)$$

Note que a última desigualde nos expressa que para todo p-primo a soma de seus expoentes em $n_1!n_2!\cdots n_s!$ é menor do que ou igual ao expoente de p-primo em $n!$. Portanto,

$$(n_1!n_2!\cdots n_s!)|n!$$

Logo,

$$\frac{n!}{n_1!n_2!\cdots n_s!}$$

é um número inteiro positivo.

2.5 UMA RELAÇÃO ENTRE AS FUNÇÕES ϕ E μ

Teorema 2.14. Seja $n \in \mathbb{Z}_+^*$. Então, é verdade que

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}.$$

Demonstração. Note que:

$$k \in \{1,\ 2,\ \ldots,\ n\} \Rightarrow \left\lfloor \frac{1}{(n,k)} \right\rfloor = \begin{cases} 1, & \text{se} \quad (n,k) = 1 \\ 0, & \text{se} \quad (n,k) > 1. \end{cases}$$

Logo, a função $\phi(n)$ pode ser expressa como

$$\phi(n) = \sum_{k=1}^{n} \left\lfloor \frac{1}{(n,k)} \right\rfloor. \tag{2.20}$$

Como, pela observação 2, $\displaystyle\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor$, então usemos este fato na equação 2.20 para obtermos:

$$\phi(n) = \sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d).$$

Como $d|(n,k)$, então $d|n$ e $d|k$, logo:

$$\phi(n) = \sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d). \tag{2.21}$$

Veja que, no último somatório da eq. 2.21, para cada divisor d de n devemos somar $\mu(d)$ somente quando os k, também, são múltiplos de d $(k = qd)$, então a variação $1 \leqslant k \leqslant n$ na soma da equação 2.21 será válida se, e somente se, $1 \leqslant q \leqslant n/d$. Logo,

$$\phi(n) = \sum_{d|n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} 1 = \sum_{d|n} \mu(d) \frac{n}{d}.$$

■

Nos Teoremas 2.8 e 2.14 demonstramos dois resultados relacionados com a função ϕ de Euler,

$$n = \sum_{d|n} \phi(n) \quad \text{e} \quad \phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

Estas duas fórmulas representam um caso especial de um importante teorema sobre a função de Möbius conhecido como *a fórmula de inversão de Möbius*, cuja será o próximo teorema a ser enunciado.

Teorema 2.15. (Fórmula de Inversão de Möbius) Sejam $n \in \mathbb{Z}_+^*$, $f(n)$ e $g(n)$ duas funções aritméticas. Se $f(n)$ e $g(n)$ satisfazem uma das seguintes condições

$$f(n) = \sum_{d|n} g(d) \quad \text{ou} \quad g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right),$$

então elas satisfazem as duas condições.

Demonstração. Suponhamos que

$$f(n) = \sum_{d|n} g(n),$$

nestas condições, vem:

$$\begin{aligned} \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{dd'=n} \mu(d) f(d') \\ &= \sum_{dd'=n} \mu(d) \sum_{m|d'} g(m) \\ &= \sum_{dmh=n} \mu(d) g(m) \\ &= \sum_{mh'=n} g(m) \sum_{d|h'} \mu(d) \end{aligned}$$

Como, pelo Teorema 2.10,

$$\sum_{d|h'} \mu(d) = \begin{cases} 1, & \text{se} \quad h' = 1 \\ 0, & \text{se} \quad h' > 1, \end{cases}$$

Logo,

$$\sum_{d|n} g(d) = f(n).$$

■

Como, pelo Teorema 2.8,

$$n = \sum_{d|n} \phi(d)$$

e as funções $f(n) = n$ e $g(n) = \phi(n)$ são ambas multiplicativas, então o Teorema 2.14 é consequência direta do Teorema 2.15.

REFERÊNCIAS

DANTE, L. R. **Matemática:** Contexto e Aplicações. v. 2. 4. ed.. São Paulo: Editora Ática, 2007.

HEFEZ, A. **Elementos de Aritmética**. 2. ed. Rio de Janeiro:IMPA, 2006.(Coleção textos universitários)

IEZZI, G. **Fundamentos de Matemática Elementar**: complexos, polinômios e equações. v. 6. 7. ed. São Paulo: Editora Atual, 2005.

LANDAU, E. G. H. **Teoria Elementar dos Números**. Rio de Janeiro: Editora Ciência Moderna, 2002.

MILIES, F. C. P. **Números:** Uma Introdução à Matemática. 3. ed. 2. reimpr. São Paulo: Editora da Universidade de São Paulo, 2006, (Acadêmica; 20).

SANTOS, J. P. O. **Introdução à Teoria dos Números**. 3. ed. Rio de Janeiro: IMPA, 2014. (Coleção matemática universitária)