Capítulo 2

Função ϕ de Euler e o princípio da inclusão e exclusão

Eldaline Rocha da Silva [1]
Rodrigo Genuino Clemente [2]

Resumo: O presente trabalho tem como propósito fazer um estudo sobre a função ϕ de Euler, que foi desenvolvida pelo matemático e físico suíço Leonhard Euler para apresentar uma generalização do Pequeno Teorema de Fermat (HEFEZ, 2011) e que mais tarde se mostrou uma importante ferramenta no desenvolvimento da Teoria dos Números. Veremos conceitos, propriedades, teoremas, demonstrações e alguns resultados importantes. Além disso, forneceremos alguns exemplos que ajudam a compreender as ideias utilizadas nas demonstrações e traremos alguns problemas não resolvidos envolvendo esta função. Para este estudo, é necessário apenas a compreensão de conteúdos vistos na educação básica, isto inclui as propriedades dos inteiros positivos relacionados com a primalidade, a divisibilidade e as operações elementares. Também apresentaremos a função de Euler interligada ao Princípio da Inclusão e Exclusão, conteúdo abordado no ensino médio.

Palavras-chave: Função Totiente de Euler; teoria dos números.

[1]UFRPE - Universidade Federal Rural de Pernambuco, eldaline_rocha@hotmail.com
[2]UFRPE - Universidade Federal Rural de Pernambuco, rodrigo.clemente@ufrpe.br

2.1 Introdução

Neste trabalho, veremos conceitos, propriedades, teoremas e alguns resultados importantes da Função ϕ de Euler, também chamada por função Totiente, usada por Leonhard Euler para provar o Pequeno Teorema de Fermat. Esta função associa a cada inteiro positivo n a quantidade de inteiros positivos menores do que n que são coprimos com n e é denotada por $\phi(n)$.

Uma outra aplicação da função ϕ é na descoberta da ordem do grupo multiplicativo de inteiros módulo n. Temos que ϕ é a cardinalidade do grupo de unidades do anel $\mathbb{Z}/n\mathbb{Z}$. Essa função também possui uma aplicação moderna em criptografia e desempenhou um papel fundamental na definição do sistema de criptografia do método RSA criado em 1977 por R. Rivest, A. Shamire e L. Adleman.

Para a compreensão deste artigo, é necessário ter o conhecimento de alguns temas referentes ao ensino básico, como, por exemplo, números primos, divisores de um número natural e operações elementares (adição, subtração, multiplicação e divisão) que são abordados desde o inicio do ensino fundamental.

Algumas definições e exemplos que serão apresentados são de fácil entendimento, possibilitando assim que o professor possa trabalhar conteúdos de nível superior com alunos da educação básica. Além disso, apresentaremos a função de Euler interligando-a com o Princípio da Inclusão e Exclusão, que é um tema visto no Ensino Médio quando se estuda Teoria dos conjuntos.

Este estudo tem como base a dissertação *Funções elementares e teoria dos números* (SILVA, 2019), que trata de algumas Funções elementares. Algumas demonstrações, mais detalhes e outros exemplos podem ser encontrados nesse trabalho. Esse material também é indicado para aprofundar-se no tema de Funções elementares e teoria dos números.

2.2 Função totiente de Euler

A função Totiente, também chamada de Função ϕ de Euler, é, na teoria dos números, definida para um número inteiro positivo n como sendo igual à quantidade de números inteiros positivos que são relativamente primos com n não excedendo n, que denotaremos por $\phi(n)$.

Foi o matemático suíço Leonhard Euler (1707-1783) que a definiu. Ele foi um dos maiores matemáticos de todos os tempos. Nascido na Suíça, era filho de um pastor protestante que esperava que ele seguisse os passos do pai. Euler possuía facilidade para o aprendizado de línguas e uma enorme habilidade para efetuar contas mentalmente.

Aos 14 anos, já ingressava na Universidade da Basileia, mas foi aos 20 anos que ganhou reconhecimento internacional, quando recebeu uma menção honrosa da Academia de Ciências de Paris. Assumiu a função de físico na nova Academia de São Petersburgo, na Rússia, em 1727, começando assim sua vida profissional. Em 1733, Euler já assumia a cátedra de matemática nesta mesma academia.

Euler produziu resultados matemáticos ao longo de sua vida. Mesmo quando a doença o assolou e ele ficou totalmente cego em 1771, isto não diminuiu a sua produtividade científica. Ele escreveu sobre vários temas como números complexos, teoria das funções, cálculo diferencial e integral, música, teoria dos números, teoria das partições e mecânica, tornando-se, assim, um dos maiores matemáticos de todos os tempos (HEFEZ, 2016).

No entanto, Euler não escolheu nenhum símbolo específico para representar esta função na época. A notação ϕ foi introduzida por Gauss no livro *Disquisitiones Arithmeticae*, publicado pela primeira vez em 1801, mas o uso do parênteses em torno do argumento não foi utilizado, sendo usada a seguinte forma: ϕn.

Foi o matemático James Joseph Sylvester que escolheu o nome Totiente, pois ele tinha o costume de inventar palavras novas para as coisas com as quais tratava. Este matemático fez contribuições nas áreas da teoria matricial, teoria dos invariantes, análise combinatória e teoria dos números.

A seguir, faremos um estudo sobre a função Totiente. Iniciaremos

apresentando a sua definição, para, em seguida, trazermos algumas de suas propriedades e exemplos. Além disso, no decorrer do trabalho, apresentaremos um estudo combinatorial desta função e a relacionaremos com o principio da inclusão e exclusão.

Definição 1. *Seja n um número natural. Definimos a função* $\phi : \mathbb{N} \to \mathbb{N}$ *dada por* $\phi(n) = |\{k \in \mathbb{N} : 1 \leq k \leq n \text{ e } mdc(k,n) = 1\}|$*, na qual* $|A|$ *indica o números de elementos de um conjunto A.*

Abaixo temos o gráfico de $\phi(n)$ para $1 \leq n \leq 1000$. Observe-se que $\phi(1) = 1$, pois o único natural menor ou igual a 1 é ele mesmo e ainda temos $\text{mdc}(1,1) = 1$. Para $n \geq 2$, temos $n = \text{mdc}(n,n) \neq 1$, de onde podemos concluir que $\phi(n) < n$.

Para encontrarmos o valor de $\phi(8)$, observemos o conjunto dos inteiros positivos que são relativamente primos com 8 não excedendo 8.
$\{x \in \mathbb{N} : 1 \leq x \leq 8 \text{ e } \text{mdc}(x,8) = 1\} = \{1,3,5,7\}$. O conjunto possui 4 elementos, assim, concluímos que $\phi(8) = 4$. Agora encontraremos o valor de $\phi(15)$.
Temos $\{x \in \mathbb{N} : 1 \leq x \leq 15 \text{ e } \text{mdc}(x,15) = 1\} = \{1,2,4,7,8,11,13,14\}$. Note que o conjunto possui 8 elementos, portanto $\phi(15) = 8$.

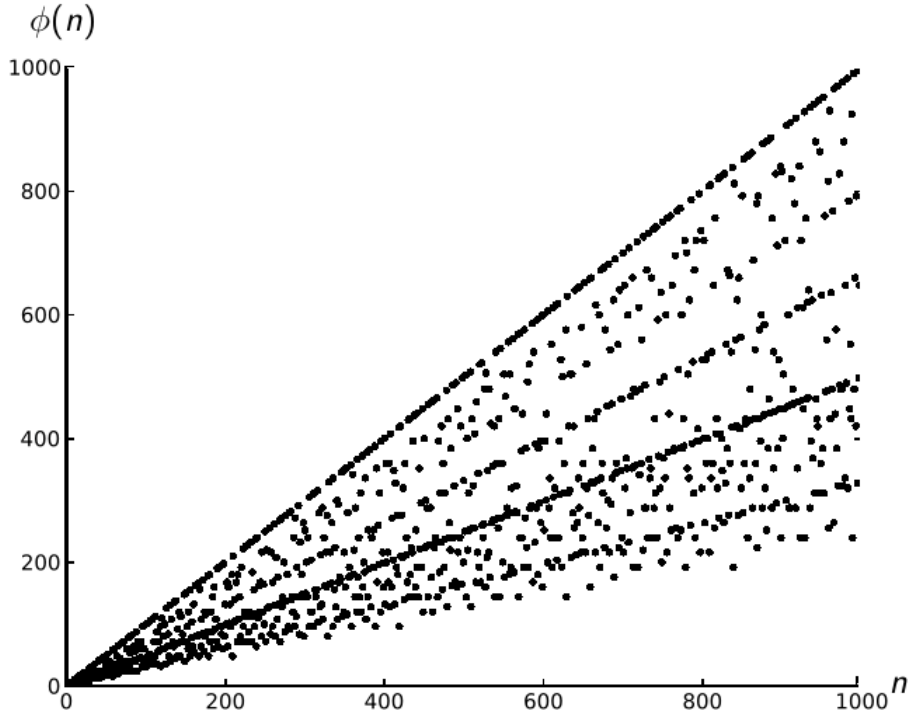
A seguir, temos duas proposições importantes e suas demonstrações.

Proposição 1. *Temos* $\phi(2) = 1$ *e* $\phi(n) \geq 2$*, para todo número natural* $n \geq 3$.

Demonstração. Temos que o único número relativamente primo com 2 e menor que 2 é o 1, logo $\phi(2) = 1$. Para $n \geq 3$ temos $n - 1 \geq 2$, como dois números consecutivos são primos entre si, segue que, para $n \geq 3$, n e $n-1$ são relativamente primos. E como $\text{mdc}(n,1) = 1$, temos 1 e $(n-1)$ coprimos com n. Logo, $\phi(n) \geq 2$ para todo número natural $n \geq 3$, como queríamos. □

Proposição 2. *Seja n um número natural, então* $\phi(n) = n - 1$*, se, e somente se, n é primo.*

Figura 2.1: Gráfico de $\phi(n)$



Fonte: Cruise (2012), editada pelo autor.

Demonstração. Suponha que $\phi(n) = n-1$, então para todo $m < n$ temos $\text{mdc}(n,m) = 1$. Logo, n não pode ser composto por um produto de fatores primos menores que n, ou seja, n é primo. Suponha que n seja primo, então todos os números naturais menores que n são relativamente primos com n, os números naturais menores que n são $1,2,3,...,n-1$, portanto $\phi(n) = n-1$, como queríamos. □

Sabemos que existem alguns tipos de números primos especiais, como, por exemplo, os *primos gêmeos*. Os primos da forma p e $p+2$ são chamados de gêmeos, denominação que foi usada pela primeira vez em 1916 pelo matemático alemão Paul Stäckel (1862 – 1919). Pela proposição anterior, é fácil mostrar que para esses primos teremos $\phi(p+2) = \phi(p)+2$. Considerando $n = p+2$ primo, temos $\phi(p+2) = (p+2)-1 = p+1 = (p-1)+2 = \phi(p)+2$.

Podemos calcular o valor de $\phi(n)$ para um natural n qualquer a partir do fato de que a função ϕ de Euler é multiplicativa, ou seja, $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$ para m e n inteiros positivos com $\text{mdc}(m,n) = 1$.

Veremos agora uma sequência de teoremas e exemplos, a fim de que consigamos calcular o valor de $\phi(n)$ para algum n relativamente grande.

Teorema 1. *Dados m e n inteiros positivos com $mdc(m,n) = 1$, então*

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

Para ilustrar o método do Teorema 1, sejam $m = 6$ e $n = 5$. Mostraremos que $\phi(5 \cdot 6) = \phi(5) \cdot \phi(6)$. Observemos a tabela abaixo contendo os números de 1 a $5 \cdot 6 = 30$

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25
26	27	28	29	30

Para encontrar os inteiros que são primos com 5, devemos observar a coluna k somente se $\text{mdc}(5,k) = 1$, ou seja, observar as colunas dos $\phi(5) = 4$ elementos que são primos com 5, então, consideraremos $k = \{1,2,3,4\}$. Na primeira linha, temos 4 elementos que são primos com 5, logo são 4 colunas para encontrarmos os elementos primos com 6. Como $\text{mdc}(5,6) = 1$, os elementos de cada coluna deixam restos diferentes quando divididos por 6, pois formam um sistema completo de resíduos módulo 6. Suponha que não se forme um sistema completo de resíduos, então pegue dois elementos quaisquer desta coluna, obedecendo a seguinte equação $(6-x) \cdot 5 + k \equiv (6-y) \cdot 5 + k \mod 6 \iff (6-x) \cdot 5 \equiv (6-y) \cdot 5 \mod 6 \iff (6-x) \equiv (6-y) \mod 6 \iff x \equiv y \mod 6$, contradição. Além disso, sabemos que $\text{mdc}(6,x) = \text{mdc}(6,r)$ onde r é o resto da divisão de x por 6, assim, em cada coluna, teremos os elementos perpassando por todos os restos de 6 (Por exemplo, na coluna

$k = 1$ teremos {1,6,11,16,21,26} que correspondem respectivamente aos restos {1,0,5,4,3,2} na divisão por 6). Logo, cada uma dessas colunas tem $\phi(6) = 2$ elementos primos com 6. Na coluna 1, temos $\{1, 11\}$; na coluna 2, {7, 17}; na coluna 3, {13, 23}; e, na coluna 4, {19, 25}. Concluímos, portanto, que $8 = \phi(5 \cdot 6) = \phi(5) \cdot \phi(6) = 4 \cdot 2$.

Uma demonstração do Teorema 1 pode ser encontrada em Silva (2019). Observe que esse Teorema não implica que os números relativamente primos com $m \cdot n$ sejam obtidos como produto dos números relativamente primos com m e os relativamente primos com n. Usemos o exemplo anterior para ilustrar $\phi(30) = \phi(5) \cdot \phi(6)$. Note que os números relativamente primos com 6 são $\{1,5\}$ e os números relativamente primos com 5 são $\{1,2,3,4\}$, enquanto que os números relativamente primos com 30 são $\{1,7,11,13,17,19,23,29\}$. Veja que há números no último conjunto que não são produtos de dois números dos outros dois conjuntos.

corolário 1. *Se m_1, m_2,...,m_r são primos entre si, dois a dois, então*

$$\phi(m_1 \cdot m_2 \cdot ... \cdot m_r) = \phi(m_1) \cdot \phi(m_2) \cdots \phi(m_r).$$

Demonstração. Demonstraremos esse corolário por indução sobre o número r de fatores. Para $r = 1$ temos $\phi(m_1) = \phi(m_1)$. Suponha que seja válido para $r = k$,

$$\phi(m_1 \cdot m_2 \cdot ... \cdot m_k) = \phi(m_1) \cdot \phi(m_2) \cdots \phi(m_k).$$

Mostraremos que é válida para $r = k + 1$. Considere m_1, m_2,...,m_k, m_{k+1} primos entre si, dois a dois. Considere $a = m_1 \cdot m_2 \cdot ... \cdot m_k$. Observe que a e m_{k+1} são primos entre si, pois $\text{mdc}(a, m_{k+1}) = mdc(m_1 \cdot m_2 \cdot ... \cdot m_k, m_{k+1}) = 1$. Como a e m_{k+1} são primos entre si, pelo Teorema 1 temos

$$\begin{aligned}
\phi(m_1 \cdot m_2 \cdot ... \cdot m_k \cdot m_{k+1}) &= \phi(a \cdot m_{k+1}) \\
&= \phi(a) \cdot \phi(m_{k+1}) \\
&= \phi(m_1 \cdot m_2 \cdot ... \cdot m_k) \cdot \phi(m_{k+1}) \\
&= \phi(m_1) \cdot \phi(m_2) \cdot ... \cdot \phi(m_k) \cdot \phi(m_{k+1})
\end{aligned}$$

Assim mostramos que a fórmula é válida para $r = k+1$, logo, por indução finita, é válida para todo número natural r. □

A partir do corolário anterior podemos afirmar que se $p_1^{\alpha_1}$, $p_2^{\alpha_2}$,...,$p_r^{\alpha_r}$ são primos entre si, dois a dois, então $\phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdot \ldots \cdot \phi(p_r^{\alpha_r})$. Demonstremos agora a fórmula para calcular $\phi(p^{\alpha})$ para cada inteiro positivo α e cada primo p.

Teorema 2. *Seja p um primo e α um inteiro positivo. Então*

$$\phi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = p^{\alpha-1} \cdot (p-1) = p^{\alpha} \cdot \left(1 - \frac{1}{p}\right).$$

Demonstração. Sabemos que $\phi(p^{\alpha})$ é a quantidade de inteiros positivos não superior a p^{α} e relativamente primos com p^{α}. Os únicos números positivos menores e que são relativamente primos com p^{α} são aqueles que não possuem o fator p. Observe que os números que possuem o fator p são os seguintes múltiplos:

$$p, 2p, 3p, \cdots, kp,$$

onde $kp = p^{\alpha}$. Logo $k = p^{\alpha-1}$. Portanto, existem $p^{\alpha-1}$ inteiros não primos com p^{α}. Portanto, $\phi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}$. □

Vamos calcular $\phi(8)$ usando o teorema demonstrado anteriormente. Temos $\phi(8) = \phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$.

Observe ainda que, pelo Corolário 1 e Teorema 2, temos:

Teorema 3. *Seja $n = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdot \ldots \cdot {p_k}^{r_k}$ a decomposição de n em fatores primos. Então $\phi(n) = {p_1}^{r_1-1} \cdot {p_2}^{r_2-1} \cdot \ldots \cdot {p_k}^{r_k-1} \cdot (p_1-1) \cdot (p_2-1) \cdot \ldots \cdot (p_k-1)$.*

A partir deste último teorema, podemos calcular facilmente o valor de $\phi(n)$ para algum n relativamente grande. Vamos fazer um exemplo. Decompondo o número 12600 em fatores primos obtemos $12600 = 2^3 \cdot 3^2 \cdot$

$5^2 \cdot 7$. Utilizando o Teorema 3, temos

$$\begin{aligned}\phi(12600) &= \phi(2^3 \cdot 3^2 \cdot 5^2 \cdot 7) \\ &= \phi(2^3) \cdot \phi(3^2) \cdot \phi(5^2) \cdot \phi(7) \\ &= 2^2(2-1) \cdot 3^1(3-1) \cdot 5^1(5-1) \cdot 7^0(7^1-1) \\ &= 4 \cdot 3 \cdot 2 \cdot 5 \cdot 4 \cdot 1 \cdot 6 \\ &= 2880\end{aligned}$$

Portanto, o número 12600 possui 2880 inteiros positivos menores que ele mesmo e que são relativamente primos com ele.

corolário 2. *Para todo número natural $n > 2$, $\phi(n)$ é par.*

Demonstração. Se a decomposição de n contém um fator primo $p \geq 3$, considere p^k a maior potência de p nesta decomposição. Podemos escrever n como o seguinte produto de fatores primos entre si $n = p^k \cdot a$. Pelos Teoremas 1 e 2, segue-se que $\phi(n) = \phi(p^k) \cdot \phi(a) = p^{k-1}(p-1) \cdot \phi(a)$. Como p é um primo maior que 3, $(p-1)$ é par, logo, $\phi(n)$ é par. Agora, se na decomposição não existir um fator primo $p \geq 3$, podemos escrever n da seguinte forma $n = 2^r$ e, como $n > 2$, temos $r > 1$, assim como $\phi(n) = \phi(2^r) = 2^{r-1}.(2-1)$. Como $r > 1$, assim $\phi(n)$ é par. □

Observemos agora os resultados abaixo para chegarmos numa nova conclusão acerca dessa função.

$$\begin{aligned}\phi(2^2) &= \phi(4) = 2 \\ \phi(2^3) &= \phi(8) = 4 \\ \phi(2^2 \cdot 2^3) &= \phi(32) = 16\end{aligned}$$

Note que $\phi(4) \cdot \phi(8) = 2 \cdot 4 < 16 = \phi(32)$. Concluímos que $\phi(2^2) \cdot \phi(2^3) < \phi(2^{2+3})$.

Ainda podemos mostrar que, para quaisquer r, s números naturais e p um número primo, teremos $\phi(p^r) \cdot \phi(p^s) < \phi(p^{r+s})$.

Teorema 4. *Se m e n são números naturais que não são primos entre si, então $\phi(m \cdot n) \neq \phi(m) \cdot \phi(n)$.*

Esse teorema e todos os resultados anteriores são obtidos a partir das propriedades multiplicativas da função ϕ de Euler. Sabemos que um número natural pode ser decomposto em um produto de fatores primos de modo único, mas pode ser escrito como a soma de dois outros números naturais de várias maneiras diferentes, por isso não se espera que ϕ tenha propriedades aditivas. Observe o seguinte exemplo para nos certificarmos:

Sabemos que $\phi(7) = 6$. Podemos decompor o número 7 das seguintes maneiras:

$$7 = 1+6, \text{ temos } \phi(7) \neq \phi(1)+\phi(6) = 1+2 = 3$$
$$7 = 2+5, \text{ temos } \phi(7) \neq \phi(2)+\phi(5) = 1+4 = 5$$
$$7 = 3+4, \text{ temos } \phi(7) \neq \phi(3)+\phi(4) = 2+2 = 4$$

Perceba que nenhumas das respostas é igual ao valor de $\phi(7)$. Além disso, note que os resultados são menores que $\phi(7)$, o que motiva a proposição seguinte:

Proposição 3. *Seja p um primo, para qualquer decomposição aditiva $p = m+n$, m e n naturais, tem-se $\phi(m)+\phi(n) < \phi(p)$.*

A partir do fato de que a função ϕ é multiplicativa e do Teorema 2, temos, a seguir, um importante resultado:

Teorema 5. *Seja $n = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdot \ldots \cdot {p_k}^{r_k}$ a decomposição de n em fatores primos.*

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right) = n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right).$$

A demonstração deste Teorema pode ser encontrada em Silva (2019). Vamos conferir dois exemplos para uma melhor compreensão. Primeiro, calculemos $\phi(15)$ de outra forma. Inicialmente encontraremos os primos presentes na fatoração de $n = 15$. Temos que $15 = 3 \cdot 5$, então:

$$\begin{aligned}\phi(15) &= 15\prod_{i=1}^{2}\left(1-\frac{1}{p_i}\right)\\ &= 15\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{5}\right)\\ &= 15\left(\frac{2}{3}\right)\cdot\left(\frac{4}{5}\right)\\ &= 8\end{aligned}$$

Então $\phi(15) = 8$, assim como foi encontrado anteriormente, quando verificamos a quantidade de elementos do conjunto $\{x \in \mathbb{N}: 1 \leq x \leq 15 \text{ e } \text{mdc}(x,15) = 1\}$.

Vamos refazer outro exemplo, calculando $\phi(n)$ para $n = 12600$ de outra forma.

Vimos que a fatoração é $12600 = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7$, então consideraremos os primos 2,3,5 e 7.

$$\begin{aligned}\phi(12600) &= 12600\prod_{i=1}^{4}\left(1-\frac{1}{p_i}\right)\\ &= 12600\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{5}\right)\cdot\left(1-\frac{1}{7}\right)\\ &= 12600\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)\left(\frac{6}{7}\right)\\ &= 2880\end{aligned}$$

Logo, confirmamos que existem 2880 números inteiros menores que 12600 e primos com ele. Fica evidente a dificuldade que teríamos para determinar todos os elementos do conjunto $\{x \in \mathbb{N}: 1 \leq x \leq n \text{ e } \text{mdc}(x,n) = 1\}$ quando n for relativamente grande. Mas, através da fórmula encontrada no Teorema 5, se torna rápido o cálculo de $\phi(n)$.

Em 1907, o matemático Robert Carmichael propôs um enigma que ainda permanece sem solução. Basicamente, Carmichael conjecturou que, para todo inteiro positivo n, há pelo menos um outro inteiro $m \neq n$ tal que $\phi(m) = \phi(n)$. Essa conjectura foi declarada em 1907, mas, como um

teorema no entanto, sua prova foi falha e em 1922 Carmichael retirou sua reivindicação e declarou a conjectura como um problema em aberto.

Tomemos, como exemplo, $\phi(m) = 4$ quando m assume um dos seguintes valores: 5,8,10 e 12. Assim, se tomarmos qualquer um desses valores como m, então qualquer um dos outros três valores pode ser usado como m, para o qual $\phi(m) = \phi(n)$.

A conjectura nos diz que, em cada caso, há mais de um valor de n com o mesmo valor de $\phi(n)$. Observa-se alguns valores na tabela a seguir:

k	Números n tais que $\phi(n) = k$	Número de soluções
1	1,2	2
2	3,4,5	3
3	5,8,10,12	4
4	7, 9, 14, 18	4
6	7, 9, 14, 18	4
8	15,16,20,24,30	5
10	11, 22	2
12	13, 21, 26, 28, 36, 42	6
16	17, 32, 34, 40, 48, 60	6

A conjectura ainda não foi mostrada como verdadeira para os inteiros pares positivos, mas podemos verificar facilmente que é verdadeira para números ímpares. Considera-se r um inteiro ímpar positivo e relembremos o fato de que $\phi(2) = 1$.

$$\phi(2r) = \phi(2)\phi(r) = \phi(r).$$

Existem alguns limites inferiores muito altos para esta conjectura. Carmichael mostrou que qualquer contra-exemplo para a conjectura deve ser pelo menos 10^{37}. Victor Klee estendeu esse resultado para 10^{400}, e um limite inferior de $10^{10^{10}}$ foi determinado por Kevin Ford em 1998.

Mais um problema não resolvido é o problema de Lehmer: existe algum número n composto tal que $\phi(n)$ divida $n-1$. Observe que para qualquer primo o problema é fácil de se resolver. Considere p um número primo, teremos $\phi(p) = p-1$ e, assim, $\phi(p)$ divide $p-1$. D. H. Lehmer

conjecturou, em 1932, que não há número composto com tal propriedade. Para esse e outros problemas não resolvidos em teoria dos números, o leitor pode consultar Guy (2013).

2.3 Estudo combinatorial de $\phi(n)$

Estudaremos, nessa seção, um teorema desenvolvido por Gauss que envolve a função ϕ de Euler. Segundo Hefez (2016), Carl Friederich Gauss (1777-1855) é um dos maiores matemáticos de todos os tempos. Nasceu na Alemanha, filho de uma família modesta, aprendeu a ler sozinho e possuía enorme habilidade para realizar cálculos mentais. Em 1799, ele demonstra o Teorema Fundamental da Álgebra, que havia sido enunciado por vários matemáticos, mas nenhuma prova correta tinha sido apresentada até então. Gauss foi um dos primeiros a tratar os números complexos dando-lhes a representação geométrica como pontos do plano cartesiano. Gauss foi também um dos criadores das geometrias não-euclidianas, da geometria diferencial, das funções de variáveis complexas, da topologia e da teoria algébrica dos números. Deu contribuições à matemática aplicada, física, astronomia e teoria das probabilidades. "Gauss teve o poder de mudar os rumos da matemática a partir dos seus trabalhos revolucionários, apresentados como extremo rigor e grande concisão e elegância. Por isso, foi considerado, pelos seus contemporâneos e pelas gerações que se sucederam, um príncipe da rainha das ciências"(HEFEZ, 2016).

Teorema 6. *(ANDREWS, 1994, Teorema 6.1)(Gauss) Considere a soma dos valores da função $\phi(n)$ para todos os d divisores de n. Então*

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

Demonstração. Seja S_n o conjunto $\{1,2,3,..,n\}$. Temos claramente que a cardinalidade de S_n é $|S_n| = n$. Para cada d que divide n, denotamos por $T_d(n)$ o conjunto de inteiros positivos não excedendo n, cujo maior divisor comum com n é d. Daí, para cada n, os conjuntos $T_d(n)$ não têm elementos

comuns. Além disso, para qualquer $m \in S_n$, vemos que $m \in T_d(n)$ onde $d = \text{mdc}(m,n)$. Consequentemente, $n = |(S_n)| = \sum_{d|n} |T_d(n)|$.

Agora, mostraremos que $T_d(n)$ tem $\phi\left(\frac{n}{d}\right)$ elementos. Primeiro, note-se que todos os elementos de $T_d(n)$ são múltiplos de d e são menores ou iguais a n. Observe-se que os únicos números da forma ad em $T_d(n)$ são aqueles para os quais $\text{mdc}(a, \frac{n}{d}) = 1$, havendo $\phi\left(\frac{n}{d}\right)$ elementos. De fato, os elementos de $T_d(n)$ são encontrados entre os números $d, 2d, \cdots, \left(\frac{n}{d}\right)d$. Agora, se $\text{mdc}\left(a, \frac{n}{d}\right) = e$, então $\text{mdc}(ad,n) = ed$ e $ed = d$ se, e somente se, $e = 1$. Assim:

$$n = |(S_n)| = \sum_{d|n} |T_d(n)| = \sum_{d|n} \phi\left(\frac{n}{d}\right).$$

Por fim, note-se que:

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

Temos que d assume os valores dos vários divisores de n e o mesmo acontece com o divisor complementar $\frac{n}{d}$. Assim, provamos nosso teorema.

Ilustremos a ideia apresentada na demonstração do Teorema 6 com exemplos. Considere $n = 6$, então d pode assumir os valores $1, 2, 3$ e 6. Teremos $T_1(6) = \{1,5\}$, $T_2(6) = \{2,4\}$, $T_3(6) = \{3\}$ e $T_6(6) = \{6\}$.

Neste exemplo, consideremos $n = 45$. Os divisores de n são: $d = 1, 3, 5, 9, 15, 45$. Separemos os números de 1 a 45 em conjuntos $T_d(n)$, cujo maior divisor comum deste número com n é d. Assim teremos:

$T_{45}(45) = \{45\}$

$T_{15}(45) = \{15, 30\}$

$T_9(45) = \{9, 18, 27, 36\}$

$T_5(45) = \{5, 10, 20, 25, 35, 40\}$

$T_3(45) = \{3, 6, 12, 21, 24, 33, 39, 42\}$

$T_1(45) = \{1, 2, 4, 7, 8, 11, 13, 14, 16, 17, 19, 22, 23, 26, 28, 29, 31, 32, 34, 37, 38, 41, 43, 44\}$

Observe que esses conjuntos são disjuntos e a união deles é o conjunto $\{1,2,3,\cdots,45\}$. Nota-se também a seguir que a quantidade de elementos em cada $T_d(45)$ é igual a $\phi(\frac{45}{d})$:

Conjuntos $T_d(n)$	Números de elementos em $T_d(n)$
$T_1(45)$	$24 = \phi(45) = \phi(\frac{45}{1})$
$T_3(45)$	$8 = \phi(15) = \phi(\frac{45}{3})$
$T_5(45)$	$6 = \phi(9) = \phi(\frac{45}{5})$
$T_9(45)$	$4 = \phi(5) = \phi(\frac{45}{9})$
$T_{15}(45)$	$2 = \phi(3) = \phi(\frac{45}{15})$
$T_{45}(45)$	$1 = \phi(1) = \phi(\frac{45}{45})$

Veja que, se d é divisor de 45, então $\frac{45}{d}$ também é. Confirmamos que $\sum_{d|n}\phi\left(\frac{n}{d}\right) = \sum_{d|n}\phi(d)$ e, além disso, temos $\sum_{d|45}\phi(d) = 45$.

2.4 Função ϕ de Euler e o princípio de inclusão e exclusão

Uma ferramenta muito importante que nos permite encontrar a resolução de vários modelos de problemas matemáticos envolvendo a contagem de elementos é o Princípio da Inclusão e Exclusão. Esse princípio nos permite calcular a quantidade de elementos que pertencem à união de conjuntos quaisquer, não necessariamente disjuntos, e será utilizado para sistematizar a fórmula da função ϕ de Euler, provada no Teorema 5.

2.4.1 Cardinalidade da união de dois conjuntos

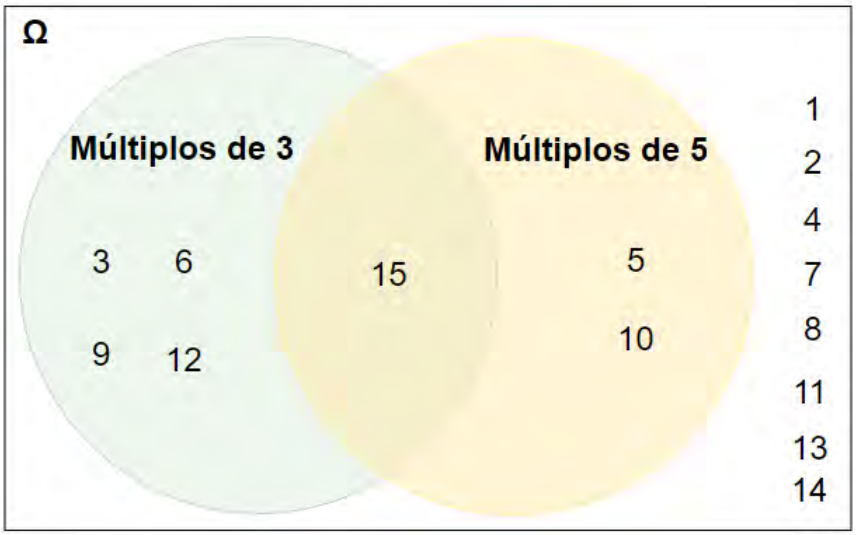
Simbolizemos por Ω o conjunto universo e $\{0\}$ o conjunto vazio. Para esta seção, utilizamos o capítulo 4 de Santos, Mello e Murari (2007), como base do nosso estudo.

Teorema 7. *Sejam A e B conjuntos finitos, então* $|A \cup B| = |A| + |B| - |A \cap B|$.

Essa é a fórmula do Princípio da Inclusão e Exclusão para dois conjuntos não disjuntos. Essa regra também tem êxito para conjuntos disjuntos, uma vez que a interseção entre conjuntos disjuntos é o conjunto vazio, então $A \cap B = \{0\}$ e $|A \cup B| = |A| + |B|$. Veremos no próximo exemplo que é possível obter $\phi(n)$, n um número natural, com facilidade e de maneira precisa pela utilização do Princípio de Inclusão e Exclusão.

Como exemplo, vamos calcular $\phi(n)$ para $n = 15$. Inicialmente devemos encontrar os p_i primos presentes na decomposição em fatores primos de n, onde $n = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdots {p_i}^{r_i}$.
Defina o conjunto $A_{p_i} = \{$números naturais menores que n e divisíveis por $p_i\}$, em seguida, devemos determinar a quantidade de elementos pertencentes a cada conjunto A_{p_i}. Para encontrarmos a quantidade de números menores ou igual a 15 e coprimos com respeito a ele, devemos encontrar a cardinalidade do complementar da união dos A_{p_i}. Observemos a figura abaixo:

Figura 2.1: Quantidade de elementos para $\phi(15)$



Fonte: Elaborada pelo autor.

Temos $n = 15 = 3 \cdot 5$, então $A_3 = \{$Múltiplos de 3$\} = \{3,6,9,12,15\}$
$A_5 = \{$Múltiplos de 5$\} = \{5,10,15\}$.
Além disso, é necessário determinar a cardinalidade da interseção destes

conjuntos: $A_3 \cap A_5 = \{\text{Múltiplos de } 15\} = \{15\}$. Observa-se que a cardinalidade de cada conjunto pode ser dada por:

$$|A_3| = \frac{15}{3} = 5$$
$$|A_5| = \frac{15}{5} = 3$$
$$|A_3 \cap A_5| = \frac{15}{5 \cdot 3} = 1$$

Tendo encontrado esses valores, podemos calcular $\phi(15)$:

$$\phi(15) = |\Omega| - |A_3 \cup A_5|$$

A partir do Teorema 7, obtemos:

$$\begin{aligned}\phi(15) &= |\Omega| - (|A_3| + |A_5| - |A_3 \cap A_5|) \\ &= 15 - (5 + 3 - 1) = 8\end{aligned}$$

2.4.2 Cardinalidade da união de três conjuntos

Para aplicarmos o Princípio da Inclusão e Exclusão a três conjuntos, devemos identificar as interseções dois a dois e a interseção entre os três conjuntos. Observa-se a seguir a fórmula que nos fornece a quantidade de elementos da união de três conjuntos:

Teorema 8. *Sejam A, B e C conjuntos finitos, então* $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

Vamos calcular a quantidade de números menores ou igual a 30 e coprimos com respeito a ele. Temos $n = 30 = 2 \cdot 3 \cdot 5$, a decomposição de n em fatores primos, então os p_i fatores primos de n, são $3, 2, 5$. Para calcularmos $\phi(n)$ para $n = 30$ por meio do Princípio da Inclusão e Exclusão, além de determinar a quantidade de elementos que pertencem a cada conjunto A_{p_i}, devemos encontrar a cardinalidade das interseções.

Observemos os conjuntos a seguir:

$$A_2 = \{2,4,6,8,10,12,14,16,18,20,22,24,26,28,30\}$$
$$A_3 = \{3,6,9,12,15,18,21,24,27,30\}$$
$$A_5 = \{5,10,15,20,25,30\}$$
$$A_2 \cap A_3 = \{6,12,18,24,30\}$$
$$A_2 \cap A_5 = \{10,20,30\}$$
$$A_3 \cap A_5 = \{15,30\}$$
$$A_2 \cap A_3 \cap A_5 = \{30\}$$

Podemos contar os elementos de cada conjunto citado, ou encontrar a cardinalidade de cada conjunto, da seguinte maneira:

$$|A_2| = \frac{30}{2} = 15$$
$$|A_3| = \frac{30}{3} = 10$$
$$|A_5| = \frac{30}{5} = 6$$
$$|A_2 \cap A_3| = \frac{30}{2 \cdot 3} = \frac{30}{6} = 5$$
$$|A_2 \cap A_5| = \frac{30}{2 \cdot 5} = \frac{30}{10} = 3$$
$$|A_3 \cap A_5| = \frac{30}{5 \cdot 3} = \frac{30}{15} = 2$$
$$|A_2 \cap A_3 \cap A_5| = \frac{30}{2 \cdot 3 \cdot 5} = \frac{30}{30} = 1$$

Os números menores ou igual a 30 e coprimos com respeito a ele são aqueles que não estão contidos nos conjuntos A_{p_i}. Portanto devemos encontrar a cardinalidade do complementar da união dos A_{p_i}. Logo:

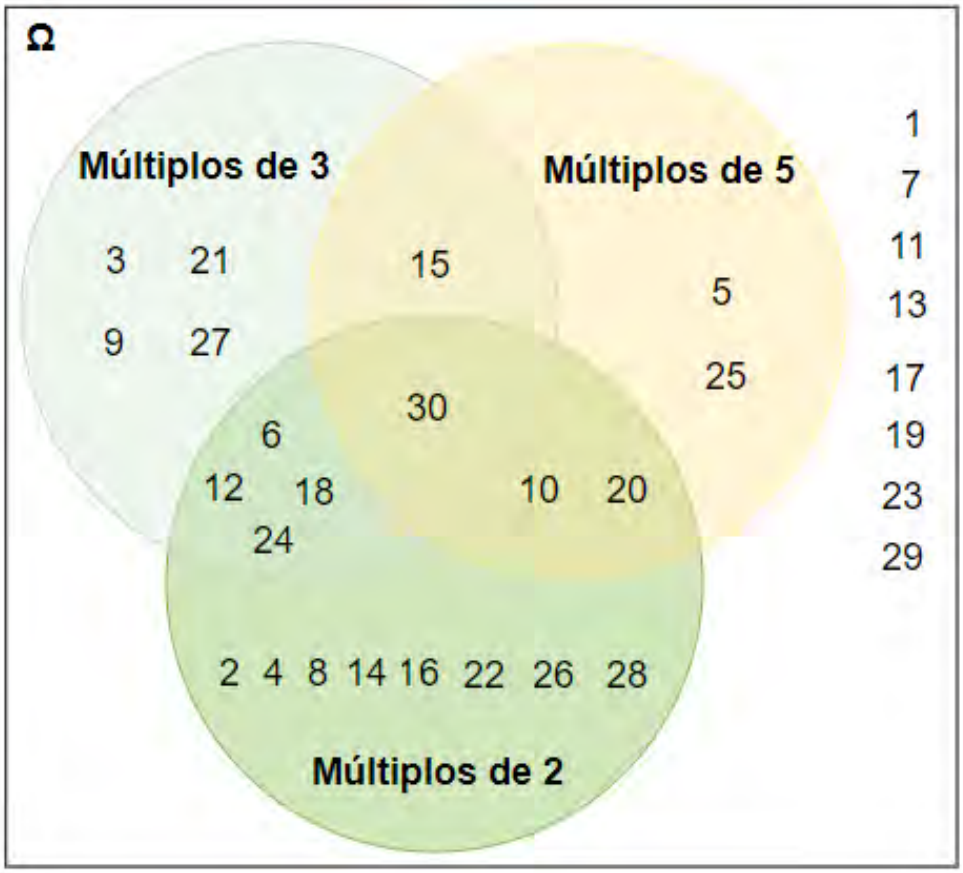
$$\phi(30) = |\Omega| - |A_2 \cup A_3 \cup A_5|$$

Onde $\Omega = \{1,2,3,\cdots,30\}$. Pelo Princípio da Inclusão e Exclusão temos

$$\begin{aligned}\phi(30) &= |\Omega| - (|A_2| + |A_3| + |A_5| - |A_2 \cap A_3| - |A_2 \cap A_5| - |A_3 \cap A_5| + |A_2 \cap A_3 \cap A_5|) \\ &= 30 - (15 + 10 + 6 - 5 - 3 - 2 + 1) = 8\end{aligned}$$

Podemos conferir nosso resultado observando a figura a seguir:

Figura 2.2: Quantidade de elementos para $\phi(30)$



Fonte: Autoria própria.

2.4.3 Princípio da inclusão e exclusão

Vimos que para definirmos a cardinalidade da união de apenas dois conjuntos se utiliza o Teorema 7 e para três conjunto o Teorema 8. A generalização para n conjuntos finitos se dá através do seguinte teorema:

Teorema 9. *(SANTOS; MELLO; MURARI, 2007, Teorema 4.1)(Princípio da Inclusão e Exclusão) Se $A_1, A_2, A_3, \cdots, A_k$ são conjuntos finitos, então:*

$$\begin{aligned}\left|\bigcup_{i=1}^{k} A_i\right| &= \sum_{1\leq i<k} |A_i| - \sum_{1\leq i<j\leq k} |A_i \cap A_j| \\ &+ \sum_{1\leq i<j<p\leq k} |A_i \cap A_j \cap A_p| - \sum_{1\leq i<j<p<q\leq k} |A_i \cap A_j \cap A_p \cap A_q| \\ &+ \cdots + (-1)^{(k-1)} |A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_k|.\end{aligned}$$

Para a demonstração deste teorema consultar Santos, Mello e Murari (2007, seção 4.2).

Usemos o Princípio da Inclusão e Exclusão para demostrar o Teorema 5, isto é, para cada $n = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdots {p_k}^{r_k}$, temos:

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Demonstração. De fato, considere $n = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdots {p_k}^{r_k}$ e defina os seguintes conjuntos:

$$\begin{aligned} A &= \{1, 2, 3, .., n\} \\ A_1 &= \{x \in A | \quad x \quad \text{é múltiplo de} \quad p_1\} \subset A \\ A_2 &= \{x \in A | \quad x \quad \text{é múltiplo de} \quad p_2\} \subset A \\ A_3 &= \{x \in A | \quad x \quad \text{é múltiplo de} \quad p_3\} \subset A \\ &\vdots \\ A_k &= \{x \in A | \quad x \quad \text{é múltiplo de} \quad p_k\} \subset A \end{aligned}$$

Como os números contidos nesses conjuntos possuem fatores primos

de n em sua fatoração, então nenhum desses é relativamente primo com n. Portanto, temos que retirar esses números do conjunto A para encontrarmos o valor de $\phi(n)$. Logo:

$$\phi(n) = |A| - |A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_k|$$

Pelo Princípio da Inclusão e Exclusão, temos:

$$\begin{aligned}\phi(n) = |A| - \Bigg| &\sum_{1\le i<k} |A_i| - \sum_{1\le i<j\le k} |A_i \cap A_j| + \sum_{1\le i<j<p\le k} |A_i \cap A_j \cap A_p| \\ &- \sum_{1\le i<j<p<q\le k} |A_i \cap A_j \cap A_p \cap A_q| + \cdots + (-1)^{(k-1)} |A_1 \cap A_2 \cap \cdots \cap A_k| \Bigg| \\ = |A| &- \sum_{1\le i<k} |A_i| - \sum_{1\le i<j\le k} |A_i \cap A_j| + \sum_{1\le i<j<p\le k} |A_i \cap A_j \cap A_p| \\ &- \sum_{1\le i<j<p<q\le k} |A_i \cap A_j \cap A_p \cap A_q| + \cdots + (-1)^{(k-1)} |A_1 \cap A_2 \cap \cdots \cap A_k|\end{aligned} \tag{2.1}$$

Sabemos que $|A| = n$ e $|A_i| = \left(\frac{n}{p_i}\right)$ para qualquer $1 \le i \le k$. Assim, para r interseções destes conjuntos, teremos:

$| \text{ A }_1 \cap A_2 \cap \cdots \cap A_r|$
$= |\{m \in N : m \le n; \quad p_{i_1} \text{ divide } m, p_{i_2} \text{ divide } m, \ldots, p_{i_r} \text{ divide } m\}$
$= \frac{n}{p_{i_1} \cdot p_{i_2} \cdots p_{i_r}}$.

Desta forma:

$$\begin{aligned}
\sum_{1\leq i<k} |A_i| &= \sum_{1\leq i<k} \left(\frac{n}{p_i}\right) \\
\sum_{1\leq i<j\leq k} |A_i \cap A_j| &= \sum_{1\leq i<j\leq k} \left(\frac{n}{p_i p_j}\right) \\
\sum_{1\leq i<j<p\leq k} |A_i \cap A_j \cap A_p| &= \sum_{1\leq i<j<p\leq k} \left(\frac{n}{p_i p_j p_p}\right) \\
\sum_{1\leq i<j<p<q\leq k} |A_i \cap A_j \cap A_p \cap A_q| &= \sum_{1\leq i<j<p<q\leq k} \left(\frac{n}{p_i p_j p_p p_q}\right) \\
&\vdots \\
|A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_k| &= \left(\frac{n}{p_1 p_2 \cdots p_k}\right).
\end{aligned}$$

Voltando para (2.1):

$$\begin{aligned}
\phi(n) &= |A| - \sum_{1\leq i<k} |A_i| - \sum_{1\leq i<j\leq k} |A_i \cap A_j| + \sum_{1\leq i<j<p\leq k} |A_i \cap A_j \cap A_p| \\
&\quad - \sum_{1\leq i<j<p<q\leq k} |A_i \cap A_j \cap A_p \cap A_q| + \cdots + (-1)^{(k-1)} |A_1 \cap A_2 \cap \cdots \cap A_k| \\
&= n - \left|\sum_{1\leq i<k} \left(\frac{n}{p_i}\right)\right| + \left|\sum_{1\leq i<j\leq k} \left(\frac{n}{p_i p_j}\right)\right| + \left|\sum_{1\leq i<j<p\leq k} \left(\frac{n}{p_i p_j p_p}\right)\right| \\
&\quad + \cdots + (-1)^{(k)} \left|\left(\frac{n}{p_1 p_2 \cdots p_k}\right)\right| \\
&= n\left[1 - \left|\sum_{1\leq i<k} \left(\frac{1}{p_i}\right)\right| + \left|\sum_{1\leq i<j\leq k} \left(\frac{1}{p_i p_j}\right)\right| + \left|\sum_{1\leq i<j<p\leq k} \left(\frac{1}{p_i p_j p_p}\right)\right| \right. \\
&\quad \left. + \cdots + (-1)^{(k)} \left|\left(\frac{1}{p_1 p_2 \cdots p_k}\right)\right|\right] \\
&= n\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
&= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right),
\end{aligned}$$

o que conclui a demonstração. □

2.5 Considerações finais

Buscamos neste artigo criar um material rico sobre a função $\phi(n)$ de Euler. Apresentamos algumas definições e exemplos que são de fácil entendimento, possibilitando assim a compreensão dos alunos do ensino médio. Desta forma, espera-se que o trabalho contribua para despertar o interesse do professor em trabalhar conteúdos de nível superior com alunos da educação básica. O estudo da função de Euler pelo Princípio da Inclusão e Exclusão, que é proposto neste trabalho, é uma possibilidade de apresentação do conteúdo para alunos a partir do primeiro ano do ensino médio.

Os alunos se deparam com teoria de números em séries do ensino básico e acabam sentindo dificuldades em desenvolver e aprimorar as habilidades que compõem o raciocínio lógico. Da perspectiva do professor, esse recebe a oportunidade de criar um ambiente na sala de aula em que a comunicação seja benéfica, propiciando momentos de interação entre alunos e professor, trocas de experiências e discussões.

Neste trabalho, buscamos oferecer uma abordagem combinatória para a teoria elementar de números, envolvendo, por exemplo, a função ϕ de Euler e o Princípio de Inclusão e Exclusão. Esses temas compartilham uma certa interseção do conhecimento comum e cada um genuinamente enriquece o outro. Desta forma, ao estudar a teoria dos números a partir de uma perspectiva combinatória, alunos e professores se beneficiam da consequente simplicidade das provas de muitos teoremas, sendo poupados de repetição e adquirindo novos insights.

2.6 Referências bibliográficas

ANDREWS, G. E. **Number Theory**. Chelmsford: Courier Corporation, 1994.

CRUISE, B. Euler's totient function. **Khan Academy**, 2012. Disponível em: <www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/euler-s-totient-function-phi-function>. Acesso em: 23 jun. 2021.

GUY, R. **Unsolved problems in number theory**. Berlin: Springer Science Business Media, 2013. v. 1.

HEFEZ, A. **Aritmética - Coleção PROFMAT**. Vol 2. Rio de Janeiro: SBM, 2016.

SANTOS, J. P. de O.; MELLO, M. P.; MURARI, I. T. C. **Introdução análise combinatória.** Rio de Janeiro: Ed. Ciência Moderna, 2007.

SILVA, E. R. **Funções elementares e teoria dos números**. 2019. Dissertação (Mestrado em Matemática) - Departamento de Matemática, Universidade Federal Rural de Pernambuco, Recife, PE. Disponível em: <dm.ufrpe.br/sites/www.dm.ufrpe.br/files/eldaline_tcc.pdf>.